4 La décomposition en facteurs premiers

Théorème 4 : Décomposition en facteurs premiers

Tout entier $a \geq 2$ s'écrit de manière unique sous la forme : $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$
avec : • $p_1, \dots p_n \in \mathbb{P}$. • $p_1 < p_2 < \dots < p_n$. • $\alpha_1, \dots, \alpha_n \in \mathbb{N}^*$
De plus, les p_i sont les diviseurs premiers de a et les α_i sont les $v_{p_i}(a)$ pour tout $i \in [\![1,n]\!]$.

Démonstration du théorème.

- *Existence*. On montre par récurrence forte sur $a \geq 2$: « a s'écrit comme un produit de nombres premiers. »
- *Si* $a = 2$. Alors a est un « produit » d'un seul nombre premier à savoir 2 (le produit est réduit à un seul terme).
- *Soit* $a \geq 2$. *Supposons la propriété vraie jusqu'au rang* a i.e. *que tout entier* $k \in [\![2,a]\!]$ *est un produit de nombres premiers. Montrons qu'alors,* $a+1$ *s'écrit aussi comme un produit de nombres premiers.*
  Deux cas sont possible :
  - Ou bien $a+1$ est premier auquel cas c'est un « produit » d'un seul nombre premier (à savoir $a+1$).
  - Ou bien $a+1$ n'est pas premier, il s'écrit ainsi $a+1 = bc$ avec $b, c \in [\![2,a]\!]$.
    L'hypothèse de récurrence assure que b et c s'écrivent comme des produits de nombres premiers.
    Il en va donc de même de l'entier $a+1 = bc$

  On a prouvé que tout entier a peut s'écrire sous la forme $a = p_1 \dots p_k$ avec $p_1, \dots, p_k \in \mathbb{P}$, non nécessairement distincts. On obtient l'écriture du théorème en regroupant les nombres identiques et en les rangeant par ordre croissant.
- *Unicité*. Supposons que : $a = q_1^{\beta_1} \dots q_m^{\beta_m}$ avec : • $q_1, \dots q_m \in \mathbb{P}$. • $q_1 < \dots < q_m$. • $\beta_1, \dots, \beta_m \in \mathbb{N}^*$

On va montrer que : • Les q_i sont les diviseurs premiers de a • Les β_i sont les valuations p_i-adiques de a
On sait déjà que les q_i sont des diviseurs premiers de a : $q_1 = p_{i_1}$, … , $q_m = p_{i_m}$ pour certains $i_1, \dots, i_m \in [\![1,n]\!]$.
Posons $J = \{i_1, \dots, i_m\}$ et pour tout $i \in [\![1,n]\!]$: (1) $\alpha_i = \beta_i$ si $i \in J$ (2) $\alpha_i = 0$ si $i \notin J$

Par conséquent : $a = \prod_{i \in J} q_i^{\beta_i} \underset{(1)}{=} \prod_{i \in J} p_i^{\alpha_i} \underset{(2)}{=} \prod_{i=1}^{n} p_i^{\alpha_i}$

Le résultat de l'exercice 6 de cours la partie IV assure que pour tout $i \in [\![1,n]\!]$: $\alpha_i = v_{p_i}(a)$.
Ceci prouve comme voulu que :
- Aucun des α_i n'est nul donc $J = [\![1,n]\!]$ et $(q_1, \dots, q_m) = (p_1, \dots, p_n)$
- Pour tout $i \in [\![1,n]\!]$: $\beta_i = \alpha_i = v_{p_i}(a)$.

Théorème 5 : Applications à la divisibilité

Soit $a, b \in \mathbb{N}^*$ et $p_1, \dots, p_n$ les facteurs premiers apparaissant dans la décomposition de a ou de b.
On peut écrire : $a = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ et $b = p_1^{\beta_1} \dots p_n^{\beta_n}$ où $\alpha_i = v_{p_i}(a)$ et $\beta_i = v_{p_i}(b)$ pour tout $i \in [\![1,n]\!]$.
1. $b \mid a$ ssi les valuations p_i-adiques de b sont inférieures à celles de a : $\forall i \in [\![1,n]\!], \quad \beta_i \leq \alpha_i$
2. • $a \wedge b = \prod_{i=1}^{n} p_i^{\min(\alpha_i, \beta_i)}$ • $a \vee b = \prod_{i=1}^{n} p_i^{\max(\alpha_i, \beta_i)}$

Démonstration .

1. *Supposons que* $b \mid a$.
   Il existe donc $k \in \mathbb{N}^*$ tel que : $a = kb$
   Soit $i \in [\![1,n]\!]$:
   $$\alpha_i = v_{p_i}(a) = v_{p_i}(kb) = \underbrace{v_{p_i}(k)}_{\geq 0} + \underbrace{v_{p_i}(b)}_{=\beta_i} \geq \beta_i$$
   Réciproquement supposons que $\beta_i \leq \alpha_i$ *pour tout* $i \in [\![1,n]\!]$.
   Alors : $p_i^{\beta_i}$ divise $p_i^{\alpha_i}$ pour tout $i \in [\![1,n]\!]$
   Ainsi : $b = \prod_{i=1}^{n} p_i^{\beta_i}$ divise $a = \prod_{i=1}^{n} p_i^{\alpha_i}$.

2. Posons : $d = \prod_{i=1}^{n} p_i^{\min(\alpha_i, \beta_i)}$
   Montrons que $d = a \wedge b$.
   - Pour tout $i \in [\![1,n]\!]$: $\min(\alpha_i, \beta_i) \leq \alpha_i$
     D'après le premier point : d divise a.
     On montre de même que d divise b.
     Par conséquent : $d \mid a \wedge b$.
   - Les diviseurs premiers de $a \wedge b$ sont des diviseurs premiers de a et b donc la décomposition en facteurs premiers de $a \wedge b$ est de la forme :
     $a \wedge b = p_1^{\gamma_1} \dots p_n^{\gamma_n}$ pour certains $\gamma_1, \dots, \gamma_n \in \mathbb{N}$
     Vu que $a \wedge b$ divise a, le premier point assure que $\gamma_i \leq \alpha_i$ pour tout $i \in [\![1,n]\!]$.
     De même : $\gamma_i \leq \beta_i$ pour tout $i \in [\![1,n]\!]$.
     Ainsi : $\gamma_i \leq \min(\alpha_i, \beta_i)$ pour tout $i \in [\![1,n]\!]$.
     Par conséquent : $a \wedge b \mid d$ (à nouveau avec le premier point).