Khôlles de Mathématiques - Semaine 18

Hugo Vangilluwen

18 Février 2024

1 L'ensemble des nombres premiers est infini

Démonstration. Notons l'ensemble des nombres premiers $\mathcal{P} = \{n \in \mathbb{N} \mid |\mathcal{D}(n) \cup \mathbb{N}| = 2\}$ Par l'absurde, supposons que $\mathcal{P}$ est fini.
Posons $m = 1 + \prod_{p \in \mathcal{P}} p \in \mathbb{N}$.
Comme $2 \in \mathcal{P}$, $m \geqslant 2$. Donc m admet un diviseur premier, $\exists q \in \mathcal{P} : q \mid m$. Donc $q \wedge m = q$.
Par ailleurs, $m = 1 + q\left(\prod_{\substack{p \in \mathcal{P} \\ p \neq q}} p\right)$. Donc $m - q\left(\prod_{\substack{p \in \mathcal{P} \\ p \neq q}} p\right) = 1$. D'après le théorème de Bézout, $q \wedge m = 1$.
Donc $q = 1$ ce qui est une contradiction avec $q \in \mathcal{P}$. □

2 Caractérisation de la valuation p-adique

Soit $n \in \mathbb{N}^*, p \in \mathcal{P}, k_0 \in \mathbb{N}$.

$$\nu_p(n) = k_0 \iff \exists m \in \mathbb{Z} : \begin{cases} n = p^{k_0} \\ m \wedge p = 1 \end{cases} \tag{1}$$

Démonstration. $\implies$ Supposons que $\nu_p(n) = k_0$.
Par définition de la valuation p-adique, $p^{\nu_p(n)} \mid n$ donc $p^{k_0} \mid n$. Notons $m \in \mathbb{Z}$ le quotient de la division euclidienne de n par p^{k_0}. Nous avons $n = p^{k_0} m$.
Comme $m \wedge p \in \mathcal{D}(p) \cap \mathbb{N}$, $m \wedge p \in \{1, p\}$. Par l'absurde, supposons que $m \wedge p = p$.

$$\begin{aligned} p \mid m &\implies \exists m' \in \mathbb{Z} : m = pm' \\ &\implies \exists m' \in \mathbb{Z} : n = pp^{k_0} m' = p^{k_0+1} m' \\ &\implies k_0 + 1 \in \left\{k \in \mathbb{N} \mid p^k | n\right\} \\ &\implies k_0 + 1 \leqslant \max\left\{k \in \mathbb{N} \mid p^k | n\right\} = \nu_p(n) = k_0 \end{aligned}$$

Ce qui est une contradiction donc $m \wedge p = 1$.
$\impliedby$ Supposons $\exists m \in \mathbb{Z} : \begin{cases} n = p^{k_0} \\ m \wedge p = 1 \end{cases}$
Par définition de la valuation p-adique, $p^{\nu_p(n)} \mid n$ donc $p^{\nu_p(n)} \mid p^{k_0} m$. Or $m \wedge p = 1$ donc $m \wedge p^{\nu_p(n)} = 1$. D'après le théorème de Gauss, $p_{\nu_p(n)} \mid p^{k_0}$. Donc $\exists \alpha \in \mathbb{Z} : \alpha p_{\nu_p(n)} = p^{k_0}$

$$\begin{aligned} \alpha p_{\nu_p(n)} = p^{k_0} &\implies p^{k_0} - \alpha p_{\nu_p(n)} = 0 \\ &\implies p^{k_0}\left(1 - \alpha p^{\nu_p(n) - k_0}\right) = 0 \text{ car } k_0 \leqslant \nu_p(n) \\ &\implies \alpha p^{\nu_p(n) - k_0} = 1 \text{ car } \mathbb{Z} \text{ est intègre} \\ &\implies p^{\nu_p(n) - k_0} \in \mathcal{D}(1) \cap \mathbb{N} \\ &\implies p^{\nu_p(n) - k_0} = 1 \\ &\implies \nu_p(n) - k_0 = 0 \\ &\implies \nu_p(n) = k_0 \end{aligned}$$

□

3 Les éléments inversibles d'un anneau A forment un groupe multiplicatif noté $(A^\times, \times)$

Démonstration. Soit $(A, +, \times)$ un anneau.
Un élément inversible (ou unité) est un élément de A symétrisable pour la loi $\times$. Posons l'ensemble des éléments inversibles $A^\times = \{a \in A \mid \exists b \in A : a \times b = b \times a = 1_A\}$.

- ⋆ Montrons que la LCI $\times$ se restreint bien à $A^\times$ en un LCI $\times_{A^\times}$.
  Soient $(a_1, a_2) \in {A^\times}^2$. Par défintion de $A^\times$, $\exists (b_1, b_2) \in A^2 : a_1 \times b_1 = b_1 \times a_1 = 1_A$ et $a_2 \times b_2 = b_2 \times a_2 = 1_A$.

$$(a_1 \times a_2) \times (b_2 \times b_1) \underbrace{=}_{\text{loi associative}} a_1 \times \underbrace{a_2 \times b_2}_{=1_A} \times b_1 = a_1 \times b_1 = 1_A$$

$$(b_2 \times b_1) \times (a_1 \times a_2) \underbrace{=}_{\text{loi associative}} b_2 \times \underbrace{b_1 \times a_1}_{=1_A} \times a_2 = b_2 \times a_2 = 1_A$$

  Donc $(a_1 \times a_2) \in A^\times$.
- ⋆ La loi $\times$ est associative donc la loi $\times_{A^\times}$ l'est aussi.
- ⋆ 1_A vérifie $1_A \times 1_A = 1_A$ donc $1_A \in A^\times$.
  De plus, $\forall a \in A^\times, 1_A \times_{A^\times} a = a \times_{A^\times} 1_A = a$ donc $\times_{A^\times}$ admet 1_A comme élément neutre.
- ⋆ Soit $a \in A^\times$. Par définition de $A^\times$, $\exists b \in A : a \times b = b \times a = 1_A$.
  D'où $b \in A^\times$. En pensant les égalités ci-dessus dans $A^\times$,

$$a \times_{A^\times} b = b \times_{A^\times} a = 1_A$$

  Donc a est inversible dans $A^\times$.

  Ainsi, $(A^\times, \times_{A^\times})$ est un groupe. □

4 L'image directe par un morphisme d'anneau d'un sous-anneau de l'anneau de départ est un sous anneau de l'anneau d'arrivée. De même pour l'image réciproque.

Démonstration. Soient $(A, +, \times)$ et $(B, +, \times)$ deux anneaux et $f : A \to B$ un morphisme d'anneau.
Soit A' un sous-anneau de A. Montrons que $f(A')$ est un sous-anneau de B.

- ⋆ Par définition de f, $f(A') \subset B$ et $(B, +, \times)$ est un anneau.
- ⋆ Soient $(u, v) \in f(A')^2$. Alors $\exists (a, b) \in {A'}^2 : f(a) = u$ et $f(b) = v$. f est un morphisme d'anneau donc un morphisme de groupe de $(A, +)$ dans $(B, +)$ donc

$$u - v = f(a) - f(b) = f(a - b)$$

  Comme A' est un sous-anneau, $a - b \in A'$. Donc $u - v \in f(A')$.
  De même, f est un morphisme d'anneau donc un morphisme de monoïde de $(A, \times)$ dans $(B, \times)$ donc

$$u \times v = f(a) \times f(b) = f(a \times b)$$

  Comme A' est un sous-anneau, $a \times b \in A'$. Donc $u \times v \in f(A')$.
- ⋆ f est un morphisme d'anneau donc $1_B = f(1_A)$. Or A' est un sous-anneau donc $1_A \in A'$. D'où $1_B \in f(A')$.

Soit B' un sous-anneau de B. Montrons que $f^{-1}(B')$ est un sous-anneau de A.

- ⋆ Par définition de f, $f^{-1}(B') \subset A$ et $(A, +, \times)$ est un anneau.
- ⋆ Soient $(a, b) \in f^{-1}(B')^2$. f est un morphisme d'anneau donc un morphisme de groupe de $(A, +)$ dans $(B, +)$ donc

$$f(a - b) = \underbrace{f(a)}_{\in B'} - \underbrace{f(b)}_{\in B'} \in B'$$

  Donc $a - b \in f^{-1}(B')$.
  De même, f est un morphisme d'anneau donc un morphisme de monoïde de $(A, \times)$ dans $(B, \times)$ donc

$$f(ab) = \underbrace{f(a)}_{\in B'} \underbrace{f(b)}_{\in B'} \in B'$$

  Donc $ab \in f^{-1}(B')$.

⋆ f est un morphisme d'anneau donc $1_B = f(1_A)$. Or B' est un sous-anneau donc $1_B \in B'$. D'où $1_A \in f^{-1}(B')$.

□