1 Formule de Mobius et dénombrements des polynômes irréductibles

Définition 1. *Soit $n \in \mathbb{N}$, on définit la fonction de Möbius $\mu : \mathbb{N} \to \mathbb{Z}$ par*

$$\mu(n) = \begin{cases} 0 & \text{si } n \text{ n'est pas produit de carrés,} \\ (-1)^k & \text{si } n \text{ est produit de } k \text{ nombres premiers distincts.} \end{cases} \tag{1}$$

Proposition 1. *Soit $n \geq 2$, alors*

$$\sum_{d|n} \mu(d) = 0. \tag{2}$$

Proof. On décompose n en produit de facteurs premiers

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}. \tag{3}$$

On peut ensuite décomposer la somme, en tenant compte que $\mu(d) = 0$ si deux diviseurs premiers divisent d,

$$\begin{aligned} \sum_{d|n} &= \mu(1) + \sum_{i=1}^{k} \mu(p_i) + \sum_{i \neq j} \mu(p_i p_j) + \ldots + \mu(p_1 \ldots p_n) && (4) \\ &= \sum_{k=0}^{n} (-1)^k \binom{n}{k} && (5) \\ &= 0. && (6) \end{aligned}$$

□