Propriétés des entiers de Peano

Associativité de l'addition : Montrons que pour tous entiers a, b et c, $a + (b + c) = (a + b) + c$. On fixe a et b et on procède par récurrence sur c :

- *Initialisation :* Pour $c = 0$, on a $a + (b + 0) = a + b = (a + b) + 0$.
- *Hérédité :* Supposons la propriété vérifiée au rang n : $a + (b + n) = (a + b) + n$, et montrons-la au rang $s(n)$. On a

$$\begin{aligned} a + (b + s(n)) &= a + s(b + n) \\ &= s(a + (b + n)) \text{ par définition de } + \\ &= s((a + b) + n) \text{ par hypothèse de récurrence} \\ &= (a + b) + s(n), \end{aligned}$$

  ce qu'il fallait démontrer.

Commutativité de l'addition : Montrons que pour tous entiers a et b, $a + b = b + a$. On procède en 3 étapes :

1. Commençons par montrer, par récurrence sur a, que $a + 0 = 0 + a$.
   - *Initialisation :* Pour $a = 0$, on a bien $0 + 0 = 0 + 0$.
   - *Hérédité :* Supposons que $n + 0 = 0 + n$ et montrons que $s(n) + 0 = 0 + s(n)$. On a $0 + s(n) = s(0 + n) = s(n + 0) = s(n) = s(n) + 0$.
2. Montrons maintenant, toujours par récurrence sur a, que pour tout p, $s(p) + a = s(p + a)$.
   - *Initialisation :* Pour $a = 0$, on a bien $s(p) + 0 = s(p) = s(p + 0)$.
   - *Hérédité :* Supposons que $s(p) + n = s(p + n)$ et montrons que $s(p) + s(n) = s(p + s(n))$. On a $s(p) + s(n) = s(s(p) + n) = s(s(p + n)) = s(p + s(n))$, comme souhaité.
3. Montrons enfin, par récurrence sur a, que pour tout $b \in \mathbb{N}$, $a + b = b + a$.
   - *Initialisation :* Pour tout $b \in \mathbb{N}$, on a bien $b + 0 = 0 + b$ d'après 1.
   - *Hérédité :* Supposons que $n + b = b + n$ et montrons que $s(n) + b = b + s(n)$. On a, d'après 2, $s(n) + b = s(n + b) = s(b + n) = b + s(n)$, comme requis.

Règle de simplification : Montrons que pour tous entiers m, n et p, si $m + n = m + p$ alors $n = p$. On procède par récurrence sur m :

- *Initialisation :* Pour $m = 0$, on a bien, si $0 + n = 0 + p$, alors $n = p$.
- *Hérédité :* Supposons que $m + n = m + p \Rightarrow n = p$, et montrons que $s(m) + n = s(m) + p \Rightarrow n = p$. On a $s(m) + n = s(m + n)$, $s(m) + p = s(m + p)$ donc $s(m) + n = s(m) + p \Rightarrow s(m + n) = s(m + p)$. Or, deux entiers différents ne peuvent avoir le même successeur : donc $m + n = m + p$, donc, par hypothèse de récurrence, $n = p$.

Somme nulle : Montrons que si $m + n = 0$ alors $m = 0$ et $n = 0$. On procède par contraposée : on montre, par récurrence sur m, que si $m \neq 0$ ou $n \neq 0$ alors $m + n \neq 0$. On procède alors par récurrence sur m :

- Si $m = 0$ alors $n \neq 0$ et $0 + n = n \neq 0$.
- Supposons que pour tout n, $m \neq 0$ ou $n \neq 0 \Rightarrow m + n \neq 0$ et montrons que pour tout n, $s(m) \neq 0$ ou $n \neq 0 \Rightarrow s(m) + n \neq 0$. Or, $s(m) + n = s(m + n)$ est le successeur de $m + n$, et 0 n'est le successeur d'aucun nombre, donc $s(m) + n \neq 0$.