

Entiers naturels

Marc Lorenzi

11 juillet 2022

I Les axiomes de Peano

I.1 Les axiomes

La théorie **PA** que nous allons étudier comporte un symbole de constante, 0, un symbole de fonction unaire S , deux symboles de fonctions binaires $+$ et $\times$, ainsi que le prédicat logique binaire $=$. Voici les axiomes :

$$(A_1) \quad Sx \neq 0$$

$$(A_2) \quad Sx = Sy \rightarrow x = y$$

$$(A_3) \quad x + 0 = x$$

$$(A_4) \quad x + Sy = S(x + y)$$

$$(A_5) \quad x \times 0 = 0$$

$$(A_6) \quad x \times Sy = x \times y + x$$

(I) Pour toute formule $\varphi(x, \vec{p})$ où la variable x n'apparaît pas liée dans φ ,

$$\frac{\varphi(0) \quad \forall x(\varphi(x) \rightarrow \varphi(Sx))}{\forall x \varphi(x)}$$

Ces axiomes ont été introduits par Dedekind et Peano, évidemment pas sous la forme ci-dessus. Leur but était de déterminer les propriétés essentielles dans la formulation de l'arithmétique. 0 représente l'entier 0 et S la fonction *successeur*, c'est à dire la fonction $x \mapsto x + 1$. Quelques remarques sur ces axiomes :

- (A_1) exprime que 0 n'est le successeur d'aucun entier.
- (A_2) exprime l'injectivité de S .
- (A_3) et (A_4) définissent l'addition.
- (A_5) et (A_6) définissent la multiplication.
- (I) est un schéma d'axiomes, le *principe d'induction mathématique*.

Propriété I.1 $(P_1) \quad x \neq 0 \rightarrow \exists y \, x = Sy$

(P_1) exprime le fait que tout entier non nul est le successeur d'un entier.

Démonstration : Soit $\varphi(x)$ la formule $x \neq 0 \rightarrow \exists y(x = Sy)$.

1.	$0 = 0$	
2.	$0 \neq 0 \rightarrow \exists y(0 = Sy)$	1
3.	$\varphi(0)$	2
4.	$\varphi(x)$	HYP
5.	$Sx = Sx$	
6.	$\exists y(Sx = Sy)$	5
7.	$\varphi(Sx)$	6
8.	$\varphi(x) \rightarrow \varphi(Sx)$	4, 7
9.	$\forall x \varphi(x)$	3, 8, I

Remarque : (A_2) et (P_1) montrent $\forall x(x \neq 0 \rightarrow \exists! y(x = Sy))$. L'unique y tel que $x = Sy$ est le *prédécesseur* de x .

I.2 Propriétés faciles

Définition I.1 (D_1) $1 \stackrel{\text{def}}{=} S0$ et $2 \stackrel{\text{def}}{=} S1$.

Propriété I.2 $1 + 1 = 2$

Démonstration :

- | | |
|-----------------------|----------|
| 1. $1 + 1 = 1 + S0$ | D_1 |
| 2. $1 + 1 = S(1 + 0)$ | $1, A_4$ |
| 3. $1 + 1 = S1$ | $2, A_3$ |
| 4. $1 + 1 = 2$ | $3, D_1$ |

Nous aurons besoin vers la fin de cet article de définir 3 et 4. Mais ne soyons pas impatients.

Propriété I.3 (P_2) $0 + x = x$

Comme, par (A_3) , on a aussi $x + 0 = x$, (P_2) exprime que 0 est le neutre pour l'addition.

Démonstration :

- | | |
|--|-----------|
| 1. $0 + 0 = 0$ | A_3 |
| 2. $0 + x = x$ | HYP |
| 3. $0 + Sx = S(0 + x)$ | A_4 |
| 4. $0 + Sx = Sx$ | $2, 3$ |
| 5. $0 + x = x \rightarrow 0 + Sx = Sx$ | $2, 4$ |
| 6. $\forall x(0 + x = x)$ | $1, 5, I$ |

Propriété I.4 (P'_2) $0 \times x = 0$

Comme, par (A_5) , on a aussi $x \times 0 = 0$, (P'_2) exprime que 0 est absorbant pour la multiplication.

Démonstration :

- | | |
|---|-----------|
| 1. $0 \times 0 = 0$ | A_5 |
| 2. $0 \times x = 0$ | hyp |
| 3. $0 \times Sx = 0 \times x + 0$ | A_6 |
| 4. $0 \times Sx = 0 + 0$ | 2 |
| 5. $0 \times Sx = 0$ | $4, A_3$ |
| 6. $0 \times x = 0 \rightarrow 0 \times Sx = 0$ | $2, 5$ |
| 7. $\forall x(0 \times x = 0)$ | $1, 6, I$ |

Propriété I.5 (P_3) $x + 1 = Sx$

Démonstration :

- | | | |
|-----|--------------------|------------|
| (1) | $x + 1 = x + S0$ | (D_1) |
| (2) | $x + 1 = S(x + 0)$ | $(1, A_4)$ |
| (3) | $x + 1 = Sx$ | $(2, A_3)$ |

Propriété I.6 (P_4) $x \times 1 = x$ et $1 \times x = x$

(P_4) exprime que 1 est le neutre de la multiplication.

Démonstration :

- | | |
|----------------------------------|----------|
| 1. $x \times 1 = x \times S0$ | D_1 |
| 2. $x \times 1 = x \times 0 + x$ | $1, A_6$ |
| 3. $x + 1 = 0 + x$ | $2, A_5$ |
| 4. $x + 1 = x$ | $3, P_2$ |

Pour la deuxième propriété, on a :

- | | |
|--|-----------|
| 1. $1 \times 0 = 0$ | A_5 |
| 2. $1 \times x = x$ | HYP |
| 3. $1 \times Sx = 1 \times x + 1$ | A_6 |
| 4. $1 \times Sx = x + 1$ | $3, 2$ |
| 5. $1 \times Sx = Sx$ | $4, P_3$ |
| 6. $1 \times x = x \rightarrow 1 \times Sx = Sx$ | $2, 5$ |
| 7. $\forall x(1 \times x = x)$ | $1, 6, I$ |

Propriété I.7 (P_5) $x + Sy = Sx + y$

Cette propriété sera fréquemment utilisée dans la suite.

Démonstration : Soit $\varphi(y)$ la formule $Sx + y = x + Sy$.

- | | | |
|-----|--------------------------------------|-------------|
| (1) | $Sx + 0 = Sx$ | (A_3) |
| (2) | $Sx + 0 = x + 1$ | $(1, P_3)$ |
| (3) | $Sx + 0 = x + S0$ | $(2, D_1)$ |
| (4) | $Sx + y = x + Sy$ | (hyp) |
| (5) | $Sx + Sy = S(x + Sy)$ | (A_4) |
| (6) | $Sx + Sy = S(Sx + y)$ | $(5, 4)$ |
| (7) | $Sx + Sy = Sx + SSy$ | $(6, A_4)$ |
| (8) | $\varphi(y) \rightarrow \varphi(Sy)$ | $(4, 7)$ |
| (9) | $\forall y \varphi(y)$ | $(1, 8, I)$ |

I.3 Résumé

- (P_1) $x \neq 0 \rightarrow \exists y(x = Sy)$
- (P_2) $0 + x = x$
- (P'_2) $0 \times x = 0$
- (P_3) $x + 1 = Sx$
- (P_4) $x \times 1 = x$ et $1 \times x = x$
- (P_5) $x + Sy = Sx + y$

II Les propriétés de l'addition

II.1 Associativité

Propriété II.1 (P_6) $(x + y) + z = x + (y + z)$

Démonstration : Soit $\varphi(z)$ la formule $\forall x \forall y ((x + y) + z = x + (y + z))$.

- $(x + y) + 0 \stackrel{A_3}{=} x + y \stackrel{A_3}{=} x + (y + 0)$. On a donc $\varphi(0)$.
- Supposons $\varphi(z)$. On a alors $(x + y) + Sz \stackrel{A_4}{=} S((x + y) + z) \stackrel{hyp}{=} S(x + (y + z)) \stackrel{A_4}{=} x + S(y + z) \stackrel{A_4}{=} x + (y + Sz)$.

Par (I), on a $\forall z \varphi(z)$.

II.2 Commutativité

Propriété II.2 (P_7) $x + y = y + x$

Démonstration : Soit $\varphi(y)$ la formule $\forall x (x + y = y + x)$.

- $x + 0 \stackrel{A_3}{=} x \stackrel{P_2}{=} 0 + x$. On a donc $\varphi(0)$.
- Supposons $\varphi(y)$. On a alors $x + Sy \stackrel{A_4}{=} S(x + y) \stackrel{hyp}{=} S(y + x) \stackrel{A_4}{=} y + Sx \stackrel{P_5}{=} Sy + x$.

Par (I), on a $\forall y \varphi(y)$.

II.3 Régularité

Propriété II.3 (P_8) $x + z = y + z \rightarrow x = y$

Démonstration : Soit $\varphi(z)$ la formule $\forall x \forall y (x + z = y + z \rightarrow x = y)$.

- Supposons $x + 0 = y + 0$. On a $x = y$ par (A_3), d'où $\varphi(0)$.
- Supposons $\varphi(z)$. Supposons $x + Sz = y + Sz$. On a donc $S(x + z) = S(y + z)$ par (A_4). Par l'axiome (A_2), $x + z = y + z$. D'où $x = y$ (hyp).

Par (I), on a $\forall z \varphi(z)$.

II.4 Résumé

- (P_6) $(x + y) + z = x + (y + z)$
- (P_7) $x + y = y + x$
- (P_8) $x + z = y + z \rightarrow x = y$

III Les propriétés de la multiplication

III.1 Distributivité

Propriété III.1 (P_9) $(x + y) \times z = x \times z + y \times z$

Démonstration : Soit $\varphi(z)$ la formule $\forall x \forall y ((x + y) \times z = x \times z + y \times z)$.

- $(x + y) \times 0 \stackrel{A_5}{=} 0$ et $x \times 0 + y \times 0 \stackrel{A_5}{=} 0 + 0 \stackrel{A_3}{=} 0$. On a donc $\varphi(0)$.
- Supposons $\varphi(z)$. On a alors $(x + y) \times Sz \stackrel{A_6}{=} (x + y) \times z + (x + y) \stackrel{hyp}{=} (x \times z + y \times z) + (x + y) \stackrel{P_6, P_7}{=} (x \times z + x) + (y \times z + y) \stackrel{A_6}{=} x \times Sz + y \times Sz$.

Par (I), on a $\forall z \varphi(z)$.

Propriété III.2 (P_{10}) $z \times (x + y) = z \times x + z \times y$

Démonstration : Soit $\varphi(y)$ la formule $\forall x \forall z (z \times (x + y) = z \times x + z \times y)$.

- $z \times (x + 0) \stackrel{A_3}{=} z \times x$ et $z \times x + z \times 0 \stackrel{A_5}{=} z \times x + 0 \stackrel{A_3}{=} z \times x$. On a donc $\varphi(0)$.

- Supposons $\varphi(y)$. On a alors $Sz \times (x + Sy) \stackrel{P_5}{=} z \times S(x + y) \stackrel{\text{hyp}}{=} z \times (x + y) + z \stackrel{\text{hyp}}{=} (z \times x + z \times y) + y \stackrel{P_6}{=} z \times x + (z \times y + y) \stackrel{A_6}{=} (z \times x + z \times Sy)$.
Par (I), on a $\forall y \varphi(y)$.

III.2 Associativité

Propriété III.3 (P_{11}) $(x \times y) \times z = x \times (y \times z)$

Démonstration : Soit $\varphi(z)$ la formule $\forall x \forall y ((x \times y) \times z = x \times (y \times z))$.

- $(x \times y) \times 0 \stackrel{A_5}{=} 0$ et $x \times (y \times 0) \stackrel{A_5}{=} x \times 0 = 0$. On a donc $\varphi(0)$.
- Supposons $\varphi(z)$. On a alors $(x \times y) \times Sz \stackrel{A_4}{=} (x \times y) \times z + x \times y \stackrel{\text{hyp}}{=} x \times (y \times z) + x \times y \stackrel{\text{hyp}}{=} x \times (y \times z + y) \stackrel{A_4}{=} x \times (y \times Sz)$.
Par (I), on a $\forall z \varphi(z)$.

III.3 Commutativité

Propriété III.4 (P_{12}) $x \times y = y \times x$

Démonstration : Soit $\varphi(y)$ la formule $\forall x (x \times y = y \times x)$.

- $x \times 0 \stackrel{A_5}{=} 0 \stackrel{??}{=} 0 \times x$. On a donc $\varphi(0)$.
- Supposons $\varphi(y)$. On a alors $x \times Sy \stackrel{A_6}{=} x \times y + x \stackrel{\text{hyp}}{=} y \times x + x \stackrel{P_9}{=} (y + 1) \times x \stackrel{P_3}{=} Sy \times x$.
Par (I), on a $\forall y \varphi(y)$.

III.4 Résumé

- (P_9) $(x + y) \times z = x \times z + y \times z$
- (P_{10}) $z \times (x + y) = z \times x + z \times y$
- (P_{11}) $(x \times y) \times z = x \times (y \times z)$
- (P_{12}) $x \times y = y \times x$

IV Une relation d'ordre

IV.1 Une relation

Définition IV.1 (D_2) $x \leq y \stackrel{\text{def}}{\iff} \exists z (y = x + z)$

On définit bien entendu $x < y$ par $(x \leq y) \wedge (x \neq y)$, $x \geq y$ par $y \leq x$ et $x > y$ par $y < x$.

IV.2 Ordre

Propriété IV.1 (P_{13}) $x \leq x$

Démonstration : Car $x \stackrel{A_3}{=} x + 0$.

Propriété IV.2 (P_{14}) $x \leq y \wedge y \leq z \rightarrow x \leq z$

Démonstration : Supposons $x \leq y$ et $y \leq z$. Il existe donc a et b tels que $y = x + a$ et $z = y + b$. On en déduit que $z \stackrel{\text{def}}{=} (x + a) + b \stackrel{P_6}{=} x + (a + b)$ donc $x \leq z$.

Lemme IV.1 (P_{15}) $x + y = 0 \rightarrow x = 0 \wedge y = 0$

Démonstration : Supposons $x + y = 0$ et $y \neq 0$. Il existe donc a tel que $y \stackrel{P_1}{=} Sa$. Mais alors $x + Sa \stackrel{A_4}{=} S(x + a) = 0$, ce qui contredit (A_1). Donc $y = 0$, puis $x = 0$ en reportant.

Corollaire IV.1 (P_{16}) $x \times y = 0 \rightarrow x = 0 \vee y = 0$

Démonstration : Supposons $x \times y = 0$ et $y \neq 0$. Il existe alors z tel que $y \stackrel{P_1}{=} Sz$. On a donc $0 = xSz \stackrel{A_6}{=} x \times z + x$. Par le lemme (P_{15}), $x \times z = 0$ et $x = 0$.

Propriété IV.3 (P_{17}) $x \leq y \wedge y \leq x \rightarrow x = y$

Démonstration : Supposons $x \leq y$ et $y \leq x$. Il existe donc a et b tels que $y = x + a$ et $x = y + b$. On en déduit que $x \stackrel{\text{hyp}}{=} y + b \stackrel{\text{hyp}}{=} (x + a) + b \stackrel{P_6}{=} x + (a + b)$. Ainsi, $x + 0 \stackrel{A_3}{=} x = x + (a + b)$. Par la régularité de l'addition (P_8), $a + b = 0$, d'où par (P_{15}) $a = b = 0$ et par (A_3) $x = y$.

IV.3 Ordre total

Propriété IV.4 (P_{18}) $x < y \leftrightarrow Sx \leq y$

Démonstration :

- ($\leftarrow$) Supposons $Sx \leq y$. On a $x \leq Sx \stackrel{P_3}{=} x + 1$. Peut-on avoir $Sx = x$? Non, car alors $x + 1 = x + 0$, d'où par (P_8) $1 \stackrel{\text{def}}{=} S0 = 0$, ce qui contredit (A_1). Donc $x < y$.
- ($\rightarrow$) Supposons $x < y$. Il existe a tel que $y \stackrel{\text{def}}{=} x + a$. Comme l'inégalité est stricte, on a $a \neq 0$, donc il existe b tel que $a \stackrel{P_1}{=} Sb$. Ainsi, $y = x + Sb \stackrel{P_5}{=} Sx + b$. Donc $Sx \leq y$.

Propriété IV.5 (P_{19}) $x \leq y \vee y \leq x$.

Démonstration : Soit $\varphi(x)$ la formule $\forall y(x \leq y \vee y \leq x)$.

- Pour tout y , $0 \leq y$ puisque $y \stackrel{A_3}{=} y + 0$. On a donc $\varphi(0)$.
- Supposons $\varphi(x)$. On a donc $y \leq x$ ou $x \leq y$. Deux cas se présentent :
 Si $y \leq x$, alors $y \leq Sx$, puisque par (P_3) $x < Sx$.
 Si $x < y$, alors $Sx \leq y$ d'après (P_{18}).

IV.4 Compatibilité de l'ordre avec l'addition

Propriété IV.6 (P_{20}) $x + z < y + z \leftrightarrow x < y$

Démonstration : Supposons $x + z < y + z$. Par (D_2) il existe $t \neq 0$ tel que $y + z = x + z + t$. Par (P_8) $y = x + t$ donc $x < y$. Inversement, supposons $x < y$. Il existe $t \neq 0$ tel que $y = x + t$. De là, $y + z = x + z + t$, donc $x + z < y + z$.

IV.5 Régularité de la multiplication

Propriété IV.7 (P_{21}) $z \neq 0 \wedge x \times z = y \times z \rightarrow x = y$

Démonstration : Supposons $x \times z = y \times z$, où $z \neq 0$. L'ordre étant total par (P_{19}), prenons par exemple $x \leq y$. Il existe donc t tel que $y = x + t$. En reportant il vient $x \times z = (x + t) \times z \stackrel{P_9}{=} x \times z + t \times z$. Par régularité de l'addition (P_8), $t \times z = 0$. Comme $z \neq 0$, on en déduit par (P_{16}) que $t = 0$, d'où par (A_3), $y = x$.

IV.6 Compatibilité de l'ordre avec la multiplication

Propriété IV.8 (P_{22}) $z \neq 0 \wedge x \times z < y \times z \leftrightarrow x < y$

Démonstration : Supposons $x < y$ et $z \neq 0$. Il existe $t \neq 0$ tel que $y = x + t$. De là, $y \times z = (x + t) \times z \stackrel{P_9}{=} x \times z + t \times z$. Mais $t \neq 0$ et $z \neq 0$, donc par (P_{16}), $t \times z \neq 0$. Ainsi, $y \times z > x \times z$.

Supposons $\neg(x < y)$ ou $z = 0$. Le cas où $z = 0$ est évident, prenons donc $z \neq 0$. On a donc $y \leq x$ car l'ordre est total par (P_{19}). Il existe donc t tel que $x = y + t$. De là, $x \times z = (y + t) \times z \stackrel{P_9}{=} y \times z + t \times z \geq y \times z$. Donc $\neg(x \times z < y \times z)$.

IV.7 Résumé

- (P_{13}) $x \leq x$
- (P_{14}) $x \leq y \wedge y \leq z \rightarrow x \leq z$
- (P_{15}) $x + y = 0 \rightarrow x = 0 \wedge y = 0$
- (P_{16}) $x \times y = 0 \rightarrow x = 0 \vee y = 0$
- (P_{17}) $x \leq y \wedge y \leq x \rightarrow x = y$
- (P_{18}) $x < y \leftrightarrow Sx \leq y$
- (P_{19}) $x \leq y \vee y \leq x$
- (P_{20}) $x + z < y + z \leftrightarrow x < y$
- (P_{21}) $z \neq 0 \wedge x \times z = y \times z \rightarrow x = y$
- (P_{22}) $z \neq 0 \wedge x \times z < y \times z \leftrightarrow x < y$

V Extensions de (I)

V.1 La récurrence forte

Propriété V.1 (SI) Pour toute formule $\varphi(x, \vec{p})$ où la variable x n'apparaît pas liée dans φ ,

$$\forall x[(\forall k(k < x \rightarrow \varphi(k, \vec{p}))) \rightarrow \varphi(x, \vec{p})] \rightarrow \forall x \varphi(x, \vec{p})$$

Démonstration : Allégeons les notations en ne faisant pas figurer le paramètre $\vec{p}$. Supposons $\forall x[(\forall k(k < x \rightarrow \varphi(k))) \rightarrow \varphi(x)]$. Soit $\psi(x)$ la formule $\forall k(k < x \rightarrow \varphi(k))$. L'hypothèse devient $\forall x(\psi(x) \rightarrow \varphi(x))$.

- On a $\psi(0)$ puisque $\neg(k < 0)$.
- Supposons $\psi(x)$. Soit $k < Sx$. On a donc $k \leq x$. Si $k < x$ on a $\varphi(k)$ par l'hypothèse $\psi(x)$. Comme $\psi(x) \rightarrow \varphi(x)$, on a aussi $\psi(k)$ si $k = x$. On a donc $\forall k(k < Sx \rightarrow \varphi(k))$. C'est à dire $\psi(Sx)$.

Par (I), on en déduit $\forall x \psi(x)$. Comme $x < Sx$ et $\psi(Sx)$, il vient $\varphi(x)$. Ainsi, $\forall x \varphi(x)$.

V.2 Bon ordre

Propriété V.2 (WO) Pour toute formule $\varphi(x, \vec{p})$ où la variable x n'apparaît pas liée dans φ ,

$$[\exists x \varphi(x, \vec{p})] \rightarrow [\exists x(\varphi(x, \vec{p}) \wedge \forall y(\varphi(y, \vec{p}) \rightarrow x \leq y))]$$

Démonstration : Allégeons les notations en ne faisant pas figurer le paramètre $\vec{p}$. Supposons $\neg(\exists x(\varphi(x) \wedge \forall y(\varphi(y) \rightarrow x \leq y)))$, c'est à dire $\forall x(\neg\varphi(x) \vee \exists y(y < x \wedge \varphi(y)))$.

Supposons $\forall k(k < x \rightarrow \neg\varphi(k))$. On n'a donc pas $\exists k(k < x \wedge \neg\varphi(k))$. Donc, on a $\neg\varphi(x)$. Par le théorème de récurrence forte, on a donc $\forall x(\neg\varphi(x))$, ou encore $\neg(\exists x \varphi(x))$. D'où le résultat par contraposition.

VI La relation « divise »

VI.1 Divisibilité

Définition VI.1 (D_3) $x|y \stackrel{\text{def}}{\iff} \exists z(y = x \times z)$

Propriété VI.1 (P_{23}) $x \times y = 1 \rightarrow x = 1 \wedge y = 1$

Démonstration : Supposons $x > 1 \vee y > 1$. Par exemple, $x > 1$. Si $y = 0$, $x \times y = 0 \neq 1$. Si $y \neq 0$, $x \times y > 1 \times y = y > 1$. Donc $x \times y \neq 1$. Par contraposition on a le résultat.

VI.2 Ordre

Propriété VI.2 (P_{24}) $x|x$

Démonstration : Car $x = x \times 1$

Propriété VI.3 (P_{25}) $x|y \wedge y|z \rightarrow x|z$

Démonstration : Supposons $x|y$ et $y|z$. Il existe donc a et b tels que $y = x \times a$ et $z = y \times b$. On a donc $z = y \times b = (x \times a) \times b = x \times (a \times b)$. Ainsi, $x|z$.

Propriété VI.4 (P_{26}) $x|y \wedge y|x \rightarrow x = y$

Démonstration : Supposons $x|y$ et $y|x$. Il existe donc a et b tels que $y = x \times a$ et $x = y \times b$. On a donc $x = y \times b = (x \times a) \times b = x \times (a \times b)$. deux cas se présentent.

- Si $x = 0$, alors $y = x \times a = 0$ donc $y = x$.
- Sinon, de $x = x \times (a \times b)$ on déduit $1 = a \times b$ par régularité de la multiplication. Donc $a = b = 1$ et $x = y$.

Propriété VI.5 (P_{27}) $x|y \wedge y \neq 0 \rightarrow x \leq y$

Démonstration : Supposons $x|y$ et $y \neq 0$. Il existe a tel que $y = x \times a$. Comme $y \neq 0$, $a \neq 0$ donc $a \geq 1$. Ainsi, $y = x \times a \geq x \times 1 = x$.

Définition VI.2 (D_4) $3 \stackrel{\text{def}}{=} S2$ et $4 \stackrel{\text{def}}{=} S3$

Propriété VI.6 $2 \times 2 = 4$

Démonstration : $2 \times 2 = 2 \times S1 = 2 \times 1 + 2 = 2 + 2 = 2 + S1 = S(2 + 1) = S3 = 4$

Propriété VI.7 (P_{28}) $\exists x \exists y (x \not\leq y \wedge y \not\leq x)$

Démonstration : Posons $3 = S2$. On a $2 < 3$ et $3 \neq 0$ donc $3 \not\leq 2$. Supposons que $2 \times a = 3$. On a alors $2 \times a < 2 \times 2$ donc $a < 2$. Mais $2 \times 0 = 0 \neq 3$ et $2 \times 1 = 2 \neq 3$. Donc $2 \not\leq 3$.

VI.3 Division euclidienne

Propriété VI.8 (P_{29}) $y \neq 0 \rightarrow \exists z (x < z \times y)$

Démonstration : Supposons $y \neq 0$. Alors $(x + 1) \times y = x \times y + y > x \times y \geq x$.

Propriété VI.9 (P_{30}) $y \neq 0 \rightarrow \exists! q (q \times y \leq x \wedge x < (q + 1) \times y)$

Démonstration :

- Soit $\varphi(z)$ la formule $z \times y > x$. La proposition précédente prouve $\exists z \varphi(z)$. Par la propriété de bon ordre, $\exists z (\varphi(z) \wedge \forall t (\varphi(t) \rightarrow z \leq t))$. Un tel z vérifie $z > 0$ puisque $z \times y > x$. Il existe donc q tel que $z = Sq$. Comme $q < z$, on n'a pas $q \times y > x$, donc $q \times y \leq x$. Et $x < z \times y = (q + 1) \times y$.
- Supposons maintenant qu'il existe q et q' vérifiant la propriété. On a $q \times y \leq x < (q' + 1) \times y$ donc $q \times y < (q' + 1) \times y$. Comme $y \neq 0$, il vient $q < q' + 1$, d'où $Sq = q + 1 \leq q' + 1$ puis $q \leq q'$. De même, $q' \leq q$, donc $q = q'$.

Propriété VI.10 (P_{31}) $y \neq 0 \rightarrow \exists! q \exists! r (x = q \times y + r \wedge r < y)$

Démonstration :

- Soit q tel que $q \times y \leq x < (q + 1) \times y$. Comme $q \times y \leq x$, on a $x = q \times y + r$. Mais alors $q \times y + r < (q + 1) \times y = q \times y + y$ d'où $r < y$.
- Supposons l'existence de q, q', r, r' tels que $x = q \times y + r = q' \times y + r'$, $r < y$ et $r' < y$. Supposons par exemple $q \leq q'$. Il existe donc z tel que $q' = q + z$. En reportant, il vient $q \times y + r = q' \times y + r' = (q + z) \times y + r' = q \times y + z \times y + r'$. Par régularité de l'addition, $r = z \times y + r'$. Mais $z \times y \leq z \times y + r' = r < y$, donc $z \times y < y$. $z \geq 1$ n'est pas acceptable, donc $z = 0$, donc $q' = q$. En reportant, il vient $r' = r$.

VI.4 Nombres premiers

Définition VI.3 (D_5) $\mathcal{P}(p) \stackrel{\text{def}}{\longleftrightarrow} p \neq 1 \wedge \forall a \forall b (p = a \times b \rightarrow a = 1 \vee b = 1)$

Propriété VI.11 (P_{32}) $x > 1 \rightarrow \exists p (\mathcal{P}(p) \wedge p|x)$

Démonstration : Soit $\varphi(x)$ la formule $x > 1 \rightarrow \exists p (\mathcal{P}(p) \wedge p|x)$. Supposons $\forall k (k < x \rightarrow \varphi(k))$. Trois cas se présentent.

- On a $x = 0$ ou $x = 1$. Alors on a trivialement $\varphi(x)$.
- On a $x > 1$ et $\mathcal{P}(x)$. Alors on a $\varphi(x)$.
- On a $x > 1$ et $\neg \mathcal{P}(x)$. Il existe donc a et b tels que $x = a \times b$ et $a > 1$ et $b > 1$. Facilement, $a < x$ donc, par l'hypothèse faite, on a $\varphi(a)$. Puisque $a > 1$, il existe p tel que $\mathcal{P}(p)$ et $p|a$. Comme $a|x$, il vient $p|x$. D'où $\varphi(x)$.
Par le principe d'induction forte, on a $\forall x \varphi(x)$.

Propriété VI.12 (P_{33}) $\exists p (\mathcal{P}(p) \wedge x < p)$

On atteint ici les limites de notre système formel. Cette proposition ne peut pas être prouvée sans faire appel à des modèles du système. Une preuve classique de cette propriété fait intervenir $(x + 1)! + 1$. Mais notre système formel ne permet pas de définir des fonctions par induction. La factorielle ne peut pas être construite.

Résumé

- $(A_1) \quad Sx \neq 0$
- $(A_2) \quad Sx = Sy \rightarrow x = y$
- $(A_3) \quad x + 0 = x$
- $(A_4) \quad x + Sy = S(x + y)$
- $(A_5) \quad x \times 0 = 0$
- $(A_6) \quad x \times Sy = x \times y + x$
- $(I) \quad \text{Pour toute formule } \varphi \text{ où la variable } x \text{ n'apparaît pas liée dans } \varphi, \varphi(0) \wedge \forall x(\varphi(x) \rightarrow \varphi(Sx)) \rightarrow \forall x(\varphi(x))$

- $(P_1) \quad x \neq 0 \rightarrow \exists y(x = Sy)$
- $(P_2) \quad 0 + x = x$
- $(P'_2) \quad 0 \times x = 0$
- $(P_3) \quad x + 1 = Sx$
- $(P_4) \quad x \times 1 = x \text{ et } 1 \times x = x$
- $(P_5) \quad x + Sy = Sx + y$
- $(P_6) \quad (x + y) + z = x + (y + z)$
- $(P_7) \quad x + y = y + x$
- $(P_8) \quad x + z = y + z \rightarrow x = y$
- $(P_9) \quad (x + y) \times z = x \times z + y \times z$
- $(P_{10}) \quad z \times (x + y) = z \times x + z \times y$
- $(P_{11}) \quad (x \times y) \times z = x \times (y \times z)$
- $(P_{12}) \quad x \times y = y \times x$
- $(P_{13}) \quad x \leq x$
- $(P_{14}) \quad x \leq y \wedge y \leq z \rightarrow x \leq z$
- $(P_{15}) \quad x + y = 0 \rightarrow x = 0 \wedge y = 0$
- $(P_{16}) \quad x \times y = 0 \rightarrow x = 0 \vee y = 0$
- $(P_{17}) \quad x \leq y \wedge y \leq x \rightarrow x = y$
- $(P_{18}) \quad x < y \leftrightarrow Sx \leq y$
- $(P_{19}) \quad x \leq y \vee y \leq x$
- $(P_{20}) \quad x + z < y + z \leftrightarrow x < y$
- $(P_{21}) \quad z \neq 0 \wedge x \times z = y \times z \rightarrow x = y$
- $(P_{22}) \quad z \neq 0 \wedge x \times z < y \times z \leftrightarrow x < y$
- $(P_{23}) \quad x \times y = 1 \rightarrow x = 1 \wedge y = 1$
- $(P_{24}) \quad x|x$
- $(P_{25}) \quad x|y \wedge y|z \rightarrow x|z$
- $(P_{26}) \quad x|y \wedge y|x \rightarrow x = y$
- $(P_{27}) \quad x|y \wedge y \neq 0 \rightarrow x \leq y$
- $(P_{28}) \quad \exists x \exists y (x \not|y \wedge y \not|x)$
- $(P_{29}) \quad y \neq 0 \rightarrow \exists z (x < z \times y)$
- $(P_{30}) \quad y \neq 0 \rightarrow \exists! q (q \times y \leq x \wedge x < (q + 1) \times y)$
- $(P_{31}) \quad y \neq 0 \rightarrow \exists! q \exists! r (x = q \times y + r \wedge r < y)$
- $(P_{32}) \quad x > 1 \rightarrow \exists p (\mathcal{P}(p) \wedge p|x)$
- $(P_{33}) \quad \exists p (\mathcal{P}(p) \wedge x < p)$

- $(D_1) \quad 1 = S0, 2 = S1.$
- $(D_2) \quad x \leq y \leftrightarrow \exists z (y = x + z)$
- $(D_3) \quad x|y \leftrightarrow \exists z (y = x \times z)$
- $(D_4) \quad 3 = S2, 4 = S3$
- $(D_5) \quad \mathcal{P}(p) \leftrightarrow p \neq 1 \wedge \forall a \forall b (p = a \times b \rightarrow a = 1 \vee b = 1)$

Dépendances jusqu'à (P_{22})

