Arithmétique de Peano

Nous étudions les axiomes qui définissent l'arithmétique usuelle des entiers naturels.

1. Les entiers naturels

1.1. Axiomatisation

L'ensemble $\mathbb{N} = \{0, 1, 2, \ldots\}$ des entiers naturels nous est familier et on en connaît beaucoup de propriétés :

$$x + 0 = x, \quad 0 + x = x, \quad x + y = y + x, \quad \ldots$$

Mais peut-on dégager ce qui fait la « substantifique moelle » de $\mathbb{N}$? Quelles sont les propriétés qui jouent le rôle d'axiomes et quelles sont celles qui peuvent être démontrées à partir de ces axiomes ? On a déjà l'habitude de procéder ainsi pour définir ce qu'est un groupe $(G, \circ)$ ou un espace vectoriel $(E, +, \cdot)$ par des définitions axiomatiques.
On va faire cette démarche pour obtenir les axiomes qui définissent l'arithmétique de $\mathbb{N}$. Il y aura sept axiomes de base (sur l'addition, la multiplication) et une série d'axiomes pour la récurrence : l'ensemble forme l'arithmétique de Peano.
Qu'est-ce qu'un axiome ? De notre point de vue, un ***axiome*** est une formule fermée. Un ensemble d'axiomes est donc une théorie. Pour un ensemble d'axiomes $\mathcal{A}$ et une formule $\mathcal{Q}$, on s'intéresse souvent à savoir si $\mathcal{A} \vdash \mathcal{Q}$. On s'intéresse aussi à l'assertion équivalente suivante (grâce au théorème de complétude) : est-ce que $\mathcal{A} \vDash \mathcal{Q}$? Mais on va surtout se placer dans une structure $\mathcal{S}$ précise et discuter si $\vDash_{\mathcal{S}} \mathcal{A}$ implique $\vDash_{\mathcal{S}} \mathcal{Q}$, c'est-à-dire, si les axiomes sont vrais dans $\mathcal{S}$, est-ce que la formule $\mathcal{Q}$ est aussi vraie dans $\mathcal{S}$? Ainsi, on va utiliser le terme *axiomes* plutôt que *théorie* car on ne cherche pas à étudier les propriétés générales des théories. On va expliciter et fixer un ensemble de formules : les axiomes de l'arithmétique de Peano qui seront notés $\mathcal{PA}$. Les entiers naturels $\mathbb{N}$ donnent un modèle de $\mathcal{PA}$, c'est-à-dire $\vDash_{\mathbb{N}} \mathcal{PA}$.

1.2. Lien avec les théorèmes d'incomplétude

Les théorèmes d'incomplétude de Gödel s'appliquent à des théories $\mathcal{T}$ suffisamment « riches ». Cela signifie concrètement que la théorie doit contenir les axiomes de Peano (c'est-à-dire $\mathcal{PA} \subset \mathcal{T}$; ou doit pouvoir les démontrer). Au final, demander qu'une théorie contienne ces axiomes n'est quand même pas une grande exigence, car il est difficile de faire des mathématiques sans avoir le droit de travailler avec les entiers.
Les entiers naturels interviendront aussi dans les chapitres suivants car la preuve des théorèmes d'incomplétude repose sur une *arithmétisation* : chaque symbole, chaque formule, chaque preuve va être encodée par un entier de $\mathbb{N}$.

1.3. Qu'est-ce que $\mathbb{N}$?

Pour chercher à axiomatiser $\mathbb{N}$, il serait bon de savoir en donner une définition. Malheureusement, ce n'est pas aussi évident.

- Une première approche est de définir un langage $\mathcal{L}$ contenant le symbole de constante 0 et une fonction « successeur » S qui joue le rôle de $S(n) = n+1$. On note alors $1 = S(0)$, $2 = S(1) = S(S(0))$, $3 = S(2)\ldots$ $\mathbb{N}$ est le plus petit ensemble pour lequel c'est possible.
- On peut aussi définir $\mathbb{N}$ à partir de la théorie des ensembles : les entiers sont construits à partir de l'ensemble vide $\varnothing$. On part d'un langage où tout objet est un ensemble (voir le chapitre « Variables et structures »).

$$\begin{aligned} 0 &= \varnothing \\ 1 &= \{\varnothing\} = \{0\} \\ 2 &= \{\varnothing, \{\varnothing\}\} = \{0, 1\} \\ 3 &= \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\} = \{0, 1, 2\} \\ &\ldots \end{aligned}$$

  On définit ainsi $S(n) = n \cup \{n\} = \{0, 1, \ldots, n\}$ désigné par $n+1$.
  On exige que 0 et les $S(n)$ soient dans l'ensemble, $\mathbb{N}$ est alors le plus petit ensemble pour lequel c'est possible. On reviendra sur ce point de vue de la théorie des ensembles lorsqu'on discutera de l'axiomatique $\mathcal{ZF}$.
- $\mathbb{N}$ peut aussi être défini de façon unique dans la logique du *second ordre*, si on écrit l'axiome de la récurrence sous la forme :

$$\forall \mathcal{P} \quad \mathcal{R}ec_{\mathcal{P}(x)}$$

  (Le principe de récurrence $\mathcal{R}ec_{\mathcal{P}(x)}$ sera défini plus tard.) Attention, on sort du cadre de la logique du premier ordre car le « pour tout » ne porte pas sur une variable individuelle, mais sur un sous-ensemble de formules, ce qui est interdit en logique du premier ordre.

Dans tous les cas, même si la définition de $\mathbb{N}$ n'est pas simple, cela correspond bien à l'ensemble que l'on connaît. Cependant, il existe aussi des modèles non standards, c'est-à-dire des ensembles qui vérifient les axiomes de Peano mais qui ne sont pas $\mathbb{N}$. On pourrait en construire à la main, mais ce sera aussi une conséquence du théorème d'incomplétude.

2. Axiomes de Peano

Les axiomes de Peano sont d'abord une liste de sept axiomes qui définissent l'arithmétique élémentaire, suivie d'un schéma d'axiomes pour le principe de récurrence.
On considère le langage du premier ordre $\mathcal{L}_0 = (0, S, +, \times)$ où :

- 0 est un symbole de constante (penser à $0 \in \mathbb{N}$).
- S est une fonction unaire, nommée ***successeur*** (penser à $S(x) = x+1$).
- $+$ est une fonction binaire (penser à l'addition).
- $\times$ est une fonction binaire (penser à la multiplication).
- $=$ est le prédicat d'égalité.

On notera $x \neq y$ pour $\neg(x = y)$. On introduira plus loin les symboles $\leqslant$ et $<$.

2.1. Arithmétique élémentaire

Voici les sept axiomes de base :

- $\mathcal{A}_1$: $\forall x \quad S(x) \neq 0$
- $\mathcal{A}_2$: $\forall x \quad (x = 0) \vee (\exists y \quad x = S(y))$
- $\mathcal{A}_3$: $\forall x \ \forall y \quad (S(x) = S(y)) \rightarrow (x = y)$
- $\mathcal{A}_4$: $\forall x \quad x + 0 = x$
- $\mathcal{A}_5$: $\forall x \ \forall y \quad x + S(y) = S(x + y)$
- $\mathcal{A}_6$: $\forall x \quad x \times 0 = 0$
- $\mathcal{A}_7$: $\forall x \ \forall y \quad x \times S(y) = (x \times y) + x$

L'ensemble de ces axiomes forme l'***arithmétique élémentaire***. On ajoutera juste après les axiomes de récurrence.
Voici des commentaires pour chacun de ces axiomes et leur interprétation dans $\mathbb{N}$:

- $\mathcal{A}_1$: Un successeur n'est jamais nul. Dans $\mathbb{N}$, on a toujours $n+1 \neq 0$. C'est important qu'on ne puisse pas revenir au point de départ, ce qui arriverait par exemple si on cyclait modulo N : $0, 1, 2, \ldots, N-1$, puis 0.
- $\mathcal{A}_2$: Tout élément non nul est un successeur. Dans $\mathbb{N}$, si $n \neq 0$ alors il existe $m \in \mathbb{N}$ tel que $n = m + 1$. (En fait « $m = n - 1$ », mais on n'a pas le droit de faire de soustraction.) Cet axiome est le seul axiome redondant car il se déduit des autres axiomes et du principe de récurrence (voir les exercices). Cependant, outre sa justification historique, il s'avérera important pour l'arithmétique $\mathcal{Q}$ de Robinson (voir en fin de chapitre).
- $\mathcal{A}_3$: Les successeurs de x et y sont égaux si et seulement si x et y sont égaux, autrement dit la fonction S est injective. Avec l'axiome $\mathcal{A}_1$, cela implique qu'en partant de 0, puis $1 = S(0)$, $2 = S(1)\ldots$ on ne crée que des nouveaux éléments. Dans $\mathbb{N}$ cela signifie $(n+1 = m+1) \rightarrow (n = m)$. Noter que par définition d'une fonction, on a toujours l'implication : si $x = y$ alors $S(x) = S(y)$.
- $\mathcal{A}_4$: Ajouter 0 (à droite) ne change rien. Dans $\mathbb{N}$, $n+0 = n$. Noter que pour l'arithmétique de Peano on prouvera que c'est aussi vrai à gauche « $0 + x = x$ », mais cela nécessite l'utilisation de la récurrence. On verra que cela devient problématique pour l'arithmétique $\mathcal{Q}$ de Robinson (voir en fin de chapitre).
- $\mathcal{A}_5$: Le successeur se comporte bien vis-à-vis de l'addition. Dans $\mathbb{N}$ on écrirait $n+(m+1) = (n+m)+1$, une conséquence de l'associativité dans $\mathbb{N}$.
- $\mathcal{A}_6$: Multiplier par 0 donne 0. Dans $\mathbb{N}$, $n \times 0 = 0$. Ce sera aussi vrai à gauche.
- $\mathcal{A}_7$: L'addition se comporte bien vis-à-vis de la multiplication. Dans $\mathbb{N}$, $n \times (m+1) = (n \times m) + n$, une conséquence de la distributivité dans $\mathbb{N}$.

2.2. Axiomes de la récurrence

On ne va pas ajouter un axiome mais une infinité d'axiomes, qu'on appelle un ***schéma d'axiomes***. Il va y avoir un axiome pour chaque formule $\mathcal{P}$ ayant x comme variable libre.
Soit $\mathcal{P}$ une formule de $\mathcal{L}_0$ ayant une variable libre x. On notera $\mathcal{P}(x)$ pour signifier la dépendance de $\mathcal{P}$ vis-à-vis de x. Cela permet aussi d'écrire $\mathcal{P}(y)$ au lieu de $\mathcal{P}[y/x]$.
Le principe de récurrence pour la formule $\mathcal{P}(x)$ s'écrit :

$$\mathcal{R}ec_{\mathcal{P}(x)} : \quad \mathcal{P}(0) \wedge \left[\forall x \quad \mathcal{P}(x) \rightarrow \mathcal{P}(S(x))\right] \quad \rightarrow \quad \forall x \ \mathcal{P}(x)$$

Dans $\mathbb{N}$, on retrouve le principe de récurrence classique :

- si $\mathcal{P}(0)$ est vraie (initialisation),
- et si $\mathcal{P}(n) \rightarrow \mathcal{P}(n+1)$ quel que soit $n \in \mathbb{N}$ (hérédité),
- alors $\mathcal{P}(n)$ est vraie pour tout $n \in \mathbb{N}$ (conclusion).

On note :

$$\mathcal{R}ec = \left\{\mathcal{R}ec_{\mathcal{P}(x)} \mid \mathcal{P} \text{ formule de } \mathcal{L}_0 \text{ ayant une variable libre } x\right\}$$

$\mathcal{R}ec$ contient une infinité (dénombrable) de formules.

Définition.
On note $\mathcal{PA} = \{\mathcal{A}_1, \dots, \mathcal{A}_7\} \cup \mathcal{R}ec$. Ce sont les axiomes de l'***arithmétique de Peano***.

Remarque.
Si on veut être un peu plus strict sur l'écriture, on peut écrire :

$$\mathcal{R}ec_{\mathcal{P}(x)} : \quad \mathcal{P}[0/x] \wedge \big(\forall y \quad \mathcal{P}[y/x] \to \mathcal{P}[S(y)/x]\big) \quad \to \quad \forall x \;\; \mathcal{P}(x)$$

En plus, si on a d'autres variables libres $x_1, \dots, x_n$, on note $\mathcal{P}(x, x_1, \dots, x_n)$ et on ajoute les quantificateurs universels au début :

$$\mathcal{R}ec_{\mathcal{P}} : \quad \forall x_1 \;\; \dots \;\; \forall x_n \;\; \Big[\mathcal{P}(0, x_1, \dots, x_n) \wedge \big[\forall x \quad \mathcal{P}(x, x_1, \dots, x_n) \to \mathcal{P}(S(x), x_1, \dots, x_n)\big] \to \forall x \;\; \mathcal{P}(x, x_1, \dots, x_n)\Big]$$

Cette version est indispensable pour prouver $x + y = y + x$ pour tout x, y en faisant une récurrence sur x.

2.3. Modèles de $\mathcal{PA}$

Proposition 1.
$\mathbb{N}$ est un modèle de $\mathcal{PA}$.

On considère la structure $\mathcal{S}$, qu'on note abusivement $\mathbb{N}$, de domaine $\mathbb{N}$, naturellement associée au langage $\mathcal{L}_0$ (0 est le zéro, $+$ est l'addition, $\times$ la multiplication et $S(n) = n+1$). On a vu dans les commentaires des axiomes que $\mathbb{N}$ vérifie les axiomes de $\mathcal{PA}$, c'est-à-dire $\vDash_{\mathbb{N}} \mathcal{A}_1, \dots, \vDash_{\mathbb{N}} \mathcal{A}_7$ et, quel que soit $\mathcal{P}$, $\vDash_{\mathbb{N}} \mathcal{R}ec_{\mathcal{P}(x)}$. Cela prouve la proposition.

Corollaire 1.
$\mathcal{PA}$ est cohérente.

On rappelle que cela signifie $\mathcal{PA} \nvdash \bot$, autrement dit, il n'existe aucune formule $\mathcal{Q}$ pour laquelle on a à la fois $\mathcal{PA} \vdash \mathcal{Q}$ et $\mathcal{PA} \vdash \neg\mathcal{Q}$. On sait qu'une théorie $\mathcal{T}$ est cohérente si et seulement si $\mathcal{T}$ admet un modèle (voir le chapitre « Théorème de complétude »). Comme $\mathbb{N}$ est un modèle de $\mathcal{PA}$, alors $\mathcal{PA}$ est cohérente.

Cependant, il existe d'autres modèles de $\mathcal{PA}$, appelés modèles ***non standards***. Ils sont tous infinis et contiennent $\mathbb{N}$. C'est un point très intéressant : à la fois notre but est d'axiomatiser $\mathbb{N}$, et effectivement on a réussi à en formaliser les propriétés essentielles ; mais en même temps on vient de dire que cela ne suffit pas à caractériser $\mathbb{N}$ de façon unique. C'est un peu paradoxal, mais ce sont ces idées qui font le cœur de ce livre. En fait, aucune axiomatisation de la logique du premier ordre ne permet de caractériser $\mathbb{N}$ de façon unique.

Avertissement. L'énoncé du premier théorème d'incomplétude de Gödel commence par l'hypothèse « Si $\mathcal{PA}$ est cohérente, … ». Pourquoi cette hypothèse, , puisqu'on vient de dire que c'est le cas ? En fait, si on se place uniquement dans le langage $\mathcal{L}_0$ de l'arithmétique de Peano, on ne peut pas prouver, à l'intérieur de ce langage, que $\mathcal{PA}$ est cohérente. C'est en fait exactement le second théorème de Gödel, qui dit qu'aucune théorie (suffisamment riche) ne peut prouver sa propre cohérence.
Ici, on admet que $\mathbb{N}$ existe. Ainsi, la théorie $\mathcal{PA}$ possède un modèle, donc elle est nécessairement cohérente. Cette certitude quant à la cohérence de $\mathcal{PA}$ repose sur une acceptation méta-mathématique de l'existence $\mathbb{N}$, c'est-à-dire qu'il faut se placer dans une théorie plus générale (par exemple $\mathcal{ZFC}$) pour confirmer cette construction.

3. Propriétés de l'arithmétique de Peano

On a défini un nombre volontairement restreint d'axiomes. Il s'agit maintenant de retrouver les propriétés arithmétiques usuelles à partir de ces axiomes. On va en prouver très peu car cela relèverait davantage d'un cours de mathématiques que d'un cours de logique. Surtout, c'est l'occasion idéale pour utiliser un logiciel de preuve formelle.

3.1. Avec les axiomes de base

Lemme 1.
$2+2=4$

Eh oui, rien n'est acquis ! On n'ose pas appeler cela un « théorème » et pourtant il faut bien justifier que $\mathcal{PA} \vdash$ « $2+2=4$ ».
Remarque. On note $1 = S(0)$, $2 = S(1)$, $3 = S(2)$, $4 = S(3)$. Ce sont juste des notations, $1, 2, 3, 4$ ne sont pas des symboles du langage mais des abréviations syntaxiques. Sans elles, il faudrait écrire $S(S(0)) + S(S(0)) = S(S(S(S(0))))$.

Démonstration.

$$\begin{aligned}
2+2 &= 2+S(1) && \text{par définition de } 2=S(1)\\
&= S(2+1) && \text{par } \mathcal{A}_5\\
&= S\big(2+S(0)\big) && \text{par définition de } 1=S(0)\\
&= S\big(S(2+0)\big) && \text{par } \mathcal{A}_5\\
&= S\big(S(2)\big) && \text{par } \mathcal{A}_4\\
&= S(3) && \text{par définition de } S(2)=3\\
&= 4 && \text{par définition de } S(3)=4
\end{aligned}$$

□

Sans la récurrence, aucune propriété algébrique générale n'est démontrable.

3.2. Avec la récurrence

Lemme 2.
$\forall x \quad 0+x=x$

Cela ressemble à l'axiome $\mathcal{A}_4$: « $\forall x \;\; x+0=x$ », mais on ne sait pas encore que l'addition est commutative.

Démonstration. Soit la formule $\mathcal{P}(x) : 0+x=x$.
Nous écrivons la preuve par récurrence dans le style mathématique classique :

- Initialisation. $\mathcal{P}(0) : 0+0=0$. C'est vrai par $\mathcal{A}_4$ (c'est le 0 à droite qui s'applique, et pas celui à gauche !).
- Hérédité. Soit n fixé. On suppose $\mathcal{P}(n)$ vraie et on doit démontrer $\mathcal{P}(S(n))$ (l'équivalent de $\mathcal{P}(n+1)$).

$$\begin{aligned}
& \mathcal{P}(n) \text{ est vraie}\\
\text{donc} \quad & 0+n=n\\
\text{donc} \quad & S(0+n)=S(n) && \text{car } S \text{ est une fonction}\\
\text{donc} \quad & 0+S(n)=S(n) && \text{par l'axiome } \mathcal{A}_5\\
\text{donc} \quad & \mathcal{P}(S(n)) \text{ est vraie.}
\end{aligned}$$

On a ainsi $\mathcal{P}(n) \to \mathcal{P}(S(n))$ et si on revient à l'écriture logique dans $\mathcal{PA}$, on a prouvé $\mathcal{P}(x) \to \mathcal{P}(S(x))$ quel que soit x.

- Conclusion. Par le principe de récurrence, ici $\mathcal{R}ec_{\mathcal{P}(x)}$, on en déduit « $\forall x \;\; \mathcal{P}(x)$ », c'est-à-dire « $\forall x \;\; 0+x=x$ ».

□

Lemme 3.
$\forall x \;\; \forall y \quad S(x)+y=S(x+y)$
C'est comme l'axiome $\mathcal{A}_5$, mais interverti.

Démonstration. Fixons x. Nous allons faire une récurrence sur la variable y. Soit $\mathcal{P}(y) : S(x)+y=S(x+y)$.

- Initialisation. $\mathcal{P}(0) : S(x)+0=S(x)=S(x+0)$. C'est vérifié.
- Hérédité. Supposons $\mathcal{P}(y)$.

$$\begin{array}{lll} & S(x)+y=S(x+y) & \text{par hypothèse de récurrence} \\ \text{donc} & S(S(x)+y)=S(S(x+y)) & \text{car } S \text{ est une fonction} \\ \text{donc} & S(x)+S(y)=S(x+S(y)) & \text{par application de } \mathcal{A}_5 \text{ à gauche et à droite} \\ \text{donc} & \mathcal{P}(S(y)) \text{ est vraie.} & \end{array}$$

  Ainsi, quel que soit y, $\mathcal{P}(y) \to \mathcal{P}(S(y))$.
- Conclusion. Par le principe de récurrence, on a $\forall y \;\; \mathcal{P}(y)$. Comme c'est valable quel que soit x, on a bien $\forall x \;\forall y \;\; S(x)+y=S(x+y)$.

Remarque. Si on voulait être rigoureux, on devrait noter $\mathcal{P}(x,y) : S(x)+y=S(x+y)$ puis prouver $\forall x \;\; \mathcal{P}(x,0)$, puis $\forall x \;\forall y \;\; \mathcal{P}(x,y) \to \mathcal{P}(x,S(y))$, ce qui conduit à $\forall x \;\forall y \;\; \mathcal{P}(x,y)$. □

Lemme 4.
$\forall x \;\; \forall y \quad x+y=y+x$
C'est la commutativité attendue de l'addition.

Démonstration. Fixons x. Nous allons faire une récurrence sur y. Soit $\mathcal{P}(y) : x+y=y+x$.

- Initialisation. $\mathcal{P}(0) : x+0=x$ (par l'axiome $\mathcal{A}_4$) et $0+x=x$ (par le Lemme 2). Donc $x+0=0+x$ est vérifié.
- Hérédité. Supposons $\mathcal{P}(y)$ vraie.

$$\begin{array}{lll} & x+y=y+x & \\ \text{donc} & S(x+y)=S(y+x) & \\ \text{donc} & x+S(y)=S(y)+x & \text{par } \mathcal{A}_5 \text{ à gauche et le Lemme 3 à droite} \\ \text{donc} & \mathcal{P}(S(y)) \text{ est vraie.} & \end{array}$$

- Conclusion. Quel que soit x : $\forall y \;\; x+y=y+x$.

□

3.3. Autres opérations

- **Non-égalité.** $x \neq y$ signifie $\neg(x=y)$.
- **Inégalité.** $x \leqslant y$ signifie $\exists z \;\; x+z=y$ (on rappelle qu'on modélise les entiers positifs, il faut penser à z comme un élément de $\mathbb{N}$).
- **Inégalité stricte.** $x<y$ signifie $(x \leqslant y) \wedge (x \neq y)$.
- Soustraction. Attention, $x-y$ n'est pas une fonction car elle n'est pas toujours bien définie, par exemple $2-3$ n'a pas de sens ici. Par contre, pour $x \leqslant y$, on sait qu'il existe z tel que $x+z=y$, on pourrait définir $y-x=z$.
- Il n'y a pas non plus une division x/y bien définie.

Il y a maintenant du travail à volonté pour démontrer par exemple :

$$(x \leqslant y) \wedge (y \leqslant z) \quad \to \quad x \leqslant z$$
$$x \leqslant y \quad \to \quad x \times z \leqslant y \times z$$
$$\dots$$

3.4. Ensembles définissables

Fixons un langage $\mathcal{L}$ du premier ordre et une structure $\mathcal{S}$ associée à $\mathcal{L}$ de domaine E.

Définition.
Un ensemble $A \subset E$ est ***définissable*** s'il existe une formule $\mathcal{P}(x)$ de $\mathcal{L}$ telle que :

$$A = \{a \in E \mid \vDash_{\mathcal{S}} \mathcal{P}(a)\}$$

Autrement dit, A est exactement l'ensemble des a pour lesquels $\mathcal{P}(a)$ est vraie.

Exemple.

- L'ensemble des nombres pairs de $\mathbb{N}$ est définissable, défini par la formule :
$$\mathcal{P}(x) : \quad \exists y \quad x = y + y$$
- Dans $\mathbb{N}$, l'ensemble des nombres premiers est définissable par la formule :
$$\mathcal{P}(x) : \quad (x \neq 1) \wedge \Big[\forall y \quad \forall z \quad (x = y \times z) \quad \to \quad (y = 1) \vee (z = 1)\Big]$$
Lorsqu'on travaille formellement dans l'arithmétique de Peano (indépendamment du modèle $\mathbb{N}$), c'est cette formule qui sert de définition à la notion de nombre premier (avec l'abréviation $1 = S(0)$).

3.5. Récurrence forte

Dans une démonstration par récurrence classique, on suppose $\mathcal{P}(n)$ pour en déduire $\mathcal{P}(n+1)$. Dans une récurrence forte, on suppose $\mathcal{P}(0), \mathcal{P}(1), \dots, \mathcal{P}(n)$ vraies pour en déduire $\mathcal{P}(n+1)$ vraie. C'est parfois très utile dans certaines démonstrations.
Voici la formule de la récurrence forte pour $\mathcal{P}$:

$$\mathcal{R}ec\mathcal{F}_{\mathcal{P}(x)} : \quad \Big[\forall x \quad \big(\forall y \quad y < x \to \mathcal{P}(y)\big) \to \mathcal{P}(x)\Big] \quad \to \quad \forall x \quad \mathcal{P}(x)$$

Sur $\mathbb{N}$, c'est bien la traduction de l'idée que l'hérédité forte $[\mathcal{P}(0) \wedge \dots \wedge \mathcal{P}(n-1)] \to \mathcal{P}(n)$ entraîne $\forall n \;\; \mathcal{P}(n)$.
L'initialisation est implicite dans cette formule. En prenant $x = 0$ dans le crochet, le terme de gauche de l'implication, « $\forall y \quad y < 0 \to \mathcal{P}(y)$ », est alors toujours vrai (car aucun y n'est strictement inférieur à 0 dans $\mathbb{N}$) ; donc $\mathcal{P}(0)$ doit être vraie afin que l'implication du crochet soit vraie.
On montrerait en exercice que la récurrence forte est en fait équivalente à la récurrence classique.

4. Autres arithmétiques

4.1. Arithmétique de Presburger

C'est une arithmétique plus simple que celle de Peano, car sans la multiplication. En effet, le langage est $\mathcal{L} = (0, S, +)$ et on considère seulement les axiomes $\mathcal{A}_1, \ldots, \mathcal{A}_5$ et $\mathcal{R}ec$. On note $\mathcal{PR}$ cette théorie. Noter que, même si la multiplication est absente, on peut définir $3x$ comme $x + x + x$, en revanche, une formule « $x \times y$ » est interdite.

Théorème 1.
$\mathcal{PR}$ est cohérente et complète.

Rappelons ce que cela signifie. Pour n'importe quelle formule $\mathcal{Q}$ (fermée) :

- $\mathcal{PR}$ est cohérente, donc ne peut pas prouver à la fois $\mathcal{Q}$ et $\neg\mathcal{Q}$.
- $\mathcal{PR}$ est complète, par conséquent $\mathcal{PR}$ prouve $\mathcal{Q}$ ou bien $\mathcal{PR}$ prouve $\neg\mathcal{Q}$.

La preuve est assez technique, elle se base sur l'« élimination des quantificateurs ». Il s'agit de transformer une formule de $\mathcal{L}$ en une formule équivalente sans quantificateur, mais en introduisant une relation d'équivalence modulo des entiers n. On transforme d'abord les $\forall$ en $\exists$, car « $\forall x \quad \mathcal{P}(x)$ » équivaut à « $\neg(\exists x \quad \neg\mathcal{P}(x))$ ». Voyons comment éliminer les quantificateurs pour l'exemple de la formule « y est pair » :

$$\exists x \quad y = x + x$$

c'est-à-dire $\exists x \quad y = 2x$, ce qui équivaut à :

$$y \equiv 0 \pmod 2$$

Ainsi, à l'aide du modulo, la formule n'a plus de quantificateurs. De façon générale, partant d'une formule fermée, on obtient une expression algébrique modulo un entier n. La formule est prouvable si et seulement si cette expression algébrique est satisfaite. Ainsi, une formule est prouvable ou bien c'est sa négation qui est prouvable.

4.2. Arithmétique $\mathcal{Q}$ de Robinson

On va définir une nouvelle axiomatique, avec addition et multiplication mais sans le principe de récurrence. On note $\mathcal{Q}$ la théorie composée des axiomes $\mathcal{A}_1, \ldots, \mathcal{A}_7$ sans ajouter d'axiomes pour la récurrence. Cette fois l'axiome $\mathcal{A}_2$ qui affirme que tout élément non nul est un successeur est indispensable.

Théorème 2.
$\mathcal{Q}$ est cohérente mais non complète.

La théorie $\mathcal{Q}$ est cohérente car $\mathbb{N}$ en est un modèle.
Pour démontrer qu'elle n'est pas complète, nous allons montrer que la formule :

$$\mathcal{G} : \quad \forall x \quad 0 + x = x$$

n'est pas démontrable, et $\neg\mathcal{G}$ non plus. (La lettre G est pour « Gödel ».)
Il ne faut pas confondre $\mathcal{G}$ avec l'axiome $\mathcal{A}_4$ « $\forall x \quad x + 0 = x$ ». Souvenez-vous que pour démontrer $\mathcal{G}$ dans le cadre de l'arithmétique de Peano, on a utilisé la récurrence, ce qui est interdit ici.

Démonstration.

- $\neg\mathcal{G}$ n'est pas prouvable.
  Par l'absurde, si $\neg\mathcal{G}$ est prouvable, alors $\mathcal{Q} \vdash \neg\mathcal{G}$. Ainsi, par le théorème de validité, on a $\mathcal{Q} \vDash \neg\mathcal{G}$. Or $\mathbb{N}$ vérifie les axiomes de $\mathcal{Q}$, c'est-à-dire $\vDash_{\mathbb{N}} \mathcal{Q}$, et donc on doit avoir $\vDash_{\mathbb{N}} \neg\mathcal{G}$. Mais dans $\mathbb{N}$, $\mathcal{G}$ est vraie, donc $\neg\mathcal{G}$ est faux. On obtient une contradiction.

- $\mathcal{G}$ n'est pas prouvable.
  On va suivre la même idée que ci-dessus. Il s'agit de trouver un modèle de $\mathcal{Q}$ dans lequel $\mathcal{G}$ est faux. Bien sûr ce modèle ne peut pas être $\mathbb{N}$, puisque dans $\mathbb{N}$, $\mathcal{G}$ est vrai.
  Soit $\mathcal{S}$ la structure de domaine $\mathbb{N} \cup \{a, b\}$. a et b sont deux objets nouveaux et distincts, on peut les considérer comme deux infinis ∞_a et ∞_b.
  Pour deux entiers, l'addition est l'addition usuelle et on pose :
  — $a + 0 = a$
  — $0 + a = b$
  On a aussi $S(a) = a$ et $S(b) = b$ (dans l'esprit « $\infty + 1 = \infty$ »), on n'a pas besoin de définir le détail des autres opérations pour la suite.
  On peut vérifier que tous les axiomes $\mathcal{A}_1, \ldots, \mathcal{A}_7$ sont satisfaits (voir les exercices). Par contre $\mathcal{G}$ est fausse, car $0 + a = b$ et $a \neq b$.
  On conclut comme précédemment. Par l'absurde, si $\mathcal{Q} \vdash \mathcal{G}$ alors $\mathcal{Q} \vDash \mathcal{G}$, donc $\vDash_{\mathcal{S}} \mathcal{G}$, donc $\mathcal{G}$ est vraie dans $\mathcal{S}$, ce qui contredit notre construction.

  □

Mais alors est-ce la fin de notre histoire ? L'objectif de Gödel et de ce livre est d'obtenir un théorème d'incomplétude et on vient de trouver une théorie incomplète. À quoi bon continuer ? La raison est la suivante : si on n'est pas content que $\mathcal{Q}$ soit incomplète car on ne sait pas démontrer $\mathcal{G}$ (ni $\neg\mathcal{G}$), on pourrait tout simplement augmenter la théorie $\mathcal{Q}$ en une théorie $\mathcal{Q}_1 = \mathcal{Q} \cup \{\mathcal{G}\}$ qui, elle, bien sûr, prouve $\mathcal{G}$. Le problème est que $\mathcal{Q}_1$ non plus n'est pas complète. Il existe $\mathcal{G}_1$ tel que ni $\mathcal{Q}_1 \vdash \mathcal{G}_1$, ni $\mathcal{Q}_1 \vdash \neg\mathcal{G}_1$ (voir les exercices). On pourrait alors considérer $\mathcal{Q}_2 = \mathcal{Q}_1 \cup \{\mathcal{G}_1\}$ … ce qui ne fait que repousser le problème. On prend alors conscience qu'il faut un énoncé général afin de justifier qu'on n'obtiendra jamais une théorie complète. C'est cela la puissance du théorème d'incomplétude de Gödel : quelle que soit la théorie, elle sera incomplète, donc ce n'est pas en ajoutant une formule non démontrable qu'on obtiendra une théorie complète.

4.3. Axiomatique $\mathcal{ZF}$ et $\mathcal{ZFC}$

La théorie de Zermelo-Fraenkel, notée $\mathcal{ZF}$, est une théorie axiomatique des ensembles qui permet, entre autres, de fonder l'arithmétique. Le langage est $\mathcal{L} = \{\in\}$ (avec égalité) et tout objet est un ensemble. Voir le chapitre « Variables et structures » pour une introduction. Ainsi, « $x \in y$ » signifie « l'ensemble x appartient à l'ensemble y ». Par exemple $\{0, 1\} \in \big\{\varnothing, \{0\}, \{1\}, \{0, 1\}\big\}$.
C'est une théorie plus moderne et beaucoup plus puissante que l'arithmétique de Peano. Cependant, nous nous en passerons pour les théorèmes d'incomplétude. Ainsi, la mini-introduction suivante à la théorie $\mathcal{ZF}$ ne sera pas utile pour la suite des chapitres.
On a déjà vu comment construire les entiers en partant de l'ensemble vide :

$$0 = \varnothing, \quad 1 = \{\varnothing\}, \quad 2 = \{\varnothing, \{\varnothing\}\} = \{0, 1\}, \quad 3 = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\} = \{0, 1, 2\}, \quad \ldots$$

et de façon plus générale $S(n) = n \cup \{n\}$.
$\mathcal{ZF}$ est régie par une liste d'axiomes permettant de manipuler les ensembles. On va en donner la liste mais pas tous les détails :

- **Axiome de l'ensemble vide** : il existe un ensemble ne contenant aucun élément.
- **Axiome de l'infini** : il garantit l'existence d'un ensemble infini (contenant tous les entiers naturels).
- **Axiome d'extensionalité** : deux ensembles ayant les mêmes éléments sont égaux.

$$\forall x \ \ \forall y \quad \big(\forall z \ (z \in x \ \leftrightarrow \ z \in y) \ \rightarrow \ x = y\big)$$

- **Axiome de fondation** : tout ensemble non vide x possède un élément y qui est disjoint de x. Cela interdit l'existence de cycles d'appartenance (comme $x \in x$).

$$\forall x \neq \varnothing \quad \exists y \in x \quad (y \cap x = \varnothing)$$

- **Axiome de la réunion** : pour un ensemble x, il existe un ensemble $\bigcup_x$ qui est la réunion de tous les ensembles appartenant à x.
$$\forall x \ \exists y \ \forall z \quad \big(z \in y \iff \exists t \ (t \in x) \wedge (z \in t)\big)$$
Par exemple, si $x = \big\{\{1,2\},\{2,3\},\{4,5\}\big\}$, alors $\bigcup_x = \{1,2,3,4,5\}$ (1, 2, ... sont considérés comme des ensembles).
- **Axiome de la paire** : à partir de deux ensembles x et y, il existe un ensemble $\{x,y\}$ exactement formé de x et de y.
Exemple : $x = \big\{\{1,2\},\{3\}\big\}$ et $y = \{3,4\}$, alors $\{x,y\} = \Big\{\big\{\{1,2\},\{3\}\big\},\{3,4\}\Big\}$. (Ce n'est pas l'union de x et y.)
- **Axiome des parties** : pour un ensemble x, il existe un ensemble $\mathcal{P}(x)$ qui est l'ensemble des parties de x. Par exemple, si $x = \{0,1\}$, alors $\mathcal{P}(x) = \big\{\varnothing,\{0\},\{1\},\{0,1\}\big\}$.
- **Schéma d'axiomes de compréhension** : ils permettent de définir des sous-ensembles à l'aide d'une formule $\mathcal{P}$: ainsi $\{x \in y \mid \mathcal{P}(x)\}$ est un ensemble.
- **Schéma d'axiomes de remplacement** : il permet de remplacer les éléments d'un ensemble par d'autres objets, le résultat reste un ensemble.

Ces axiomes forment la théorie $\mathcal{ZF}$.

On considère souvent en plus l'axiome suivant :

- **Axiome du choix** $\mathcal{AC}$: pour tout ensemble A, il existe une fonction qui à chaque partie non vide de A, associe un élément de cette partie.

Cet axiome est indépendant de $\mathcal{ZF}$ (on ne peut ni le démontrer, ni démontrer sa négation à partir de $\mathcal{ZF}$) ce qui fait qu'on peut l'ajouter ou non selon ses besoins quand on est confronté à des ensembles infinis. Il se retrouve sous des formes différentes (lemme de Zorn, théorème de Krull), il est indispensable pour certaines démonstrations classiques (existence de bases dans des espaces vectoriels de dimension infinie, existence de parties de $\mathbb{R}$ non mesurables au sens de Lebesgue) et peut aussi simplifier certaines démonstrations (théorème de Hahn-Banach dans le cas dénombrable). Si on décide d'adopter l'axiome du choix, on note la théorie $\mathcal{ZFC}$. C'est le cadre classique des mathématiques modernes.