Calcul sur ordinateur avec les nombres p-adiques

Xavier Caruso
Université Rennes 1
xavier.caruso@normalesup.org

Journées **N**ationales de
Calcul **F**ormel

16 au 20 janvier 2017

Première partie

Introduction aux nombres p-adiques

Que sont les nombres p-adiques ?

Que sont les nombres p-adiques ?

p — nombre premier fixé

Que sont les nombres p-adiques ?

p — nombre premier fixé

Dans les exemples, on prendra toujours $p = 2$

Que sont les nombres p-adiques ?

p — nombre premier fixé

Dans les exemples, on prendra toujours $p = 2$

Les entiers p-adiques

Que sont les nombres p-adiques ?

p — nombre premier fixé

Dans les exemples, on prendra toujours $p = 2$

Les entiers p-adiques

$$\overline{\ldots a_n a_{n-1} \ldots a_2 a_1 a_0}^{(p)}$$

Que sont les nombres p-adiques ?

p — nombre premier fixé

Dans les exemples, on prendra toujours $p = 2$

Les entiers p-adiques

$$\overline{\ldots a_n a_{n-1} \ldots a_2 a_1 a_0}^{(p)}$$
$$= a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1} + a_n p^n + \cdots$$

Que sont les nombres p-adiques ?

p — nombre premier fixé

Dans les exemples, on prendra toujours $p = 2$

Les entiers p-adiques

$$\begin{aligned} &\ldots a_n a_{n-1} \ldots a_2 a_1 a_0 \\ &= a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1} + a_n p^n + \cdots \end{aligned}$$

Que sont les nombres p-adiques ?

p — nombre premier fixé

Dans les exemples, on prendra toujours $p = 2$

Les entiers p-adiques

$$\begin{aligned} &\ldots a_n a_{n-1} \ldots a_2 a_1 a_0 \\ &= a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1} + a_n p^n + \cdots \end{aligned}$$

Les nombres p-adiques

Que sont les nombres p-adiques ?

p — nombre premier fixé

Dans les exemples, on prendra toujours $p = 2$

Les entiers p-adiques

$$\begin{aligned} &\ldots a_n a_{n-1} \ldots a_2 a_1 a_0 \\ &= a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1} + a_n p^n + \cdots \end{aligned}$$

Les nombres p-adiques

$$\overline{\ldots a_n a_{n-1} \ldots a_2 a_1 a_0 \quad , \quad a_{-1} a_{-2} \ldots a_{-v}}^{(p)}$$

Que sont les nombres p-adiques ?

p — nombre premier fixé

Dans les exemples, on prendra toujours $p = 2$

Les entiers p-adiques

$$\begin{aligned} &\ldots a_n a_{n-1} \ldots a_2 a_1 a_0 \\ &= a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1} + a_n p^n + \cdots \end{aligned}$$

Les nombres p-adiques

$$\begin{aligned} &\overline{\ldots a_n a_{n-1} \ldots a_2 a_1 a_0 \quad , \quad a_{-1} a_{-2} \ldots a_{-v}}^{(p)} \\ &= a_{-v} p^{-v} + \cdots + a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n + \cdots \end{aligned}$$

Que sont les nombres p-adiques ?

p — nombre premier fixé

Dans les exemples, on prendra toujours $p = 2$

Les entiers p-adiques

$$\begin{aligned} &\ldots a_n a_{n-1} \ldots a_2 a_1 a_0 \\ &= a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1} + a_n p^n + \cdots \end{aligned}$$

Les nombres p-adiques

$$\begin{aligned} &\ldots a_n a_{n-1} \ldots a_2 a_1 a_0 \quad , \quad a_{-1} a_{-2} \ldots a_{-v} \\ &= a_{-v} p^{-v} + \cdots + a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n + \cdots \end{aligned}$$

Structure d’anneau

Structure d’anneau

Addition

Structure d'anneau

Addition

$$
\begin{array}{cccccccccccc}
\cdots & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
\cdots & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
\hline
\end{array}
$$

Structure d'anneau

Addition

$$
\begin{array}{cccccccccccc}
\cdots & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
\cdots & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
\hline
 & & & & & & & & & & 1
\end{array}
$$

Structure d'anneau

Addition

$$
\begin{array}{cccccccccccc}
\cdots & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
\cdots & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
\hline
 & & & & & & & & & 1 & 1
\end{array}
$$

Structure d'anneau

Addition

$$
\begin{array}{cccccccccc}
\cdots & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
\cdots & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
\hline
 & & & & & & & & 0 & 1 & 1
\end{array}
$$

Structure d'anneau

Addition

$$
\begin{array}{cccccccccc}
\cdots & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
\cdots & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
\hline
 & & & & & & & 0 & 0 & 1 & 1
\end{array}
$$

Structure d'anneau

Addition

$$
\begin{array}{cccccccccccc}
 & & & & & & 1 & & & & & \\
\cdots & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
\cdots & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
\hline
 & & & & & & 0 & 0 & 0 & 1 & 1
\end{array}
$$

Structure d'anneau

Addition

$$
\begin{array}{cccccccccc}
 & & & & 1 & 1 & & & & \\
\cdots & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
\cdots & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
\hline
 & & & & & 1 & 0 & 0 & 0 & 1 & 1
\end{array}
$$

Structure d'anneau

Addition

$$
\begin{array}{cccccccccccc}
 & & & & 1 & 1 & 1 & & & & & \\
\cdots & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
\cdots & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
\hline
 & & & & 0 & 1 & 0 & 0 & 0 & 1 & 1
\end{array}
$$

Structure d'anneau

Addition

$$
\begin{array}{cccccccccc}
 & & 1 & 1 & 1 & 1 & & & & \\
\cdots & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
\cdots & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
\hline
 & & & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1
\end{array}
$$

Structure d'anneau

Addition

$$
\begin{array}{cccccccccc}
 & & \scriptstyle 1 & \scriptstyle 1 & \scriptstyle 1 & \scriptstyle 1 & & & & \\
\cdots & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
\cdots & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
\hline
 & & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1
\end{array}
$$

Structure d'anneau

Addition

$$
\begin{array}{cccccccccc}
 & & 1 & 1 & 1 & 1 & & & & \\
\cdots & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
\cdots & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
\hline
 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1
\end{array}
$$

Structure d'anneau

Addition

$$
\begin{array}{cccccccccc}
 & & 1 & 1 & 1 & 1 & & & & \\
\cdots & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
\cdots & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
\hline
\cdots & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1
\end{array}
$$

Structure d'anneau

Addition

$$
\begin{array}{cccccccccc}
 & & 1 & 1 & 1 & 1 & & & & \\
\cdots & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
\cdots & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
\hline
\cdots & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1
\end{array}
$$

Soustraction

Structure d'anneau

Addition

$$
\begin{array}{cccccccccc}
 & & 1 & 1 & 1 & 1 & & & & \\
\cdots & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
\cdots & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
\hline
\cdots & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1
\end{array}
$$

Soustraction

$$
\begin{array}{cccccccccc}
\cdots & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
\cdots & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
\hline
\end{array}
$$

Structure d'anneau

Addition

$$
\begin{array}{cccccccccccc}
 & & & \overset{1}{} & \overset{1}{} & \overset{1}{} & \overset{1}{} & & & & & \\
\cdots & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
\cdots & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
\hline
\cdots & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1
\end{array}
$$

Soustraction

$$
\begin{array}{cccccccccccc}
\cdots & 0 & {}_{1}0 & {}_{1}1 & {}_{1}0 & 1 & 1 & 0 & 0 & 1 & {}_{1}0 \\
\cdots & {}^{1+}1 & {}^{1+}0 & {}^{1+}1 & 1 & 1 & 1 & 0 & 0 & {}^{1+}0 & 1 \\
\hline
\cdots & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}
$$

Structure d’anneau

Multiplication

Structure d'anneau

Multiplication

$$
\begin{array}{cccccccccc}
\cdots & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
\cdots & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
\hline
\cdots & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
\cdots & 1 & 1 & 0 & 0 & 1 & 0 & & & & \\
\cdots & 1 & 0 & 0 & 1 & 0 & & & & & \\
\cdots & 0 & 0 & 1 & 0 & & & & & & \\
\cdots & 0 & 1 & 0 & & & & & & & \\
\cdots & 0 & & & & & & & & & \\
\hline
\cdots & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0
\end{array}
$$

Structure de corps

Division

Structure de corps

Division

Structure de corps

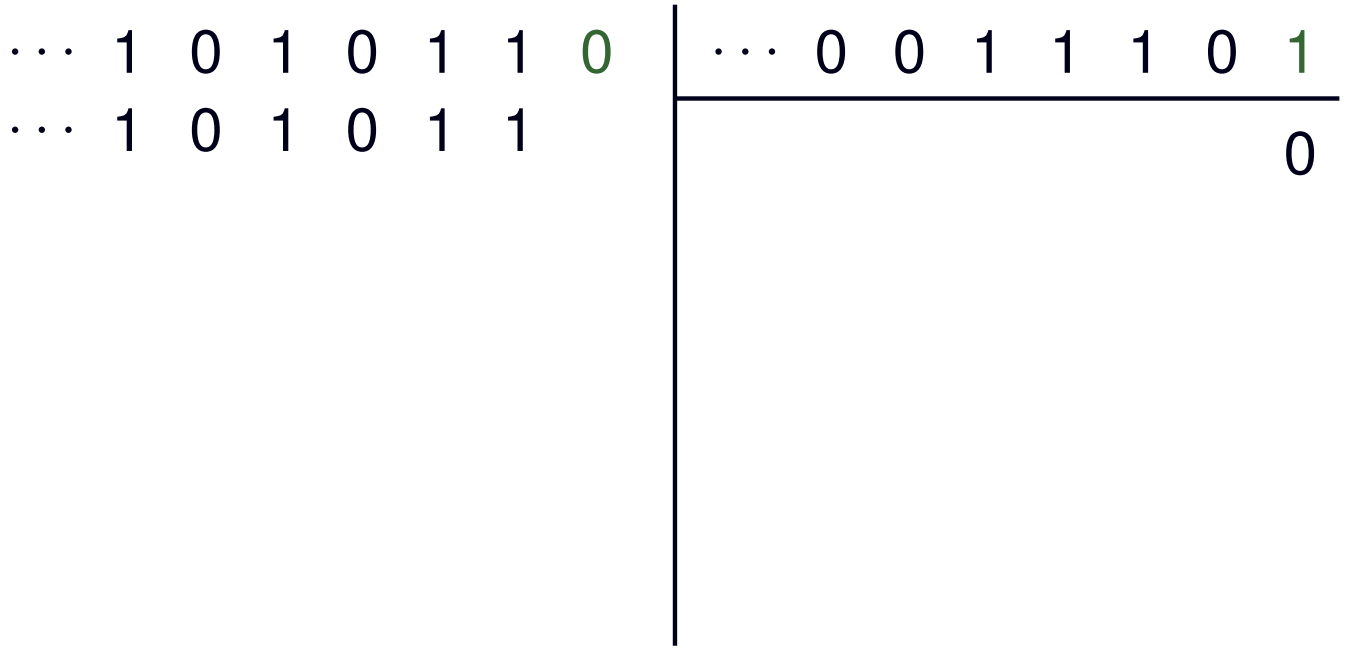
Division

Structure de corps

Division

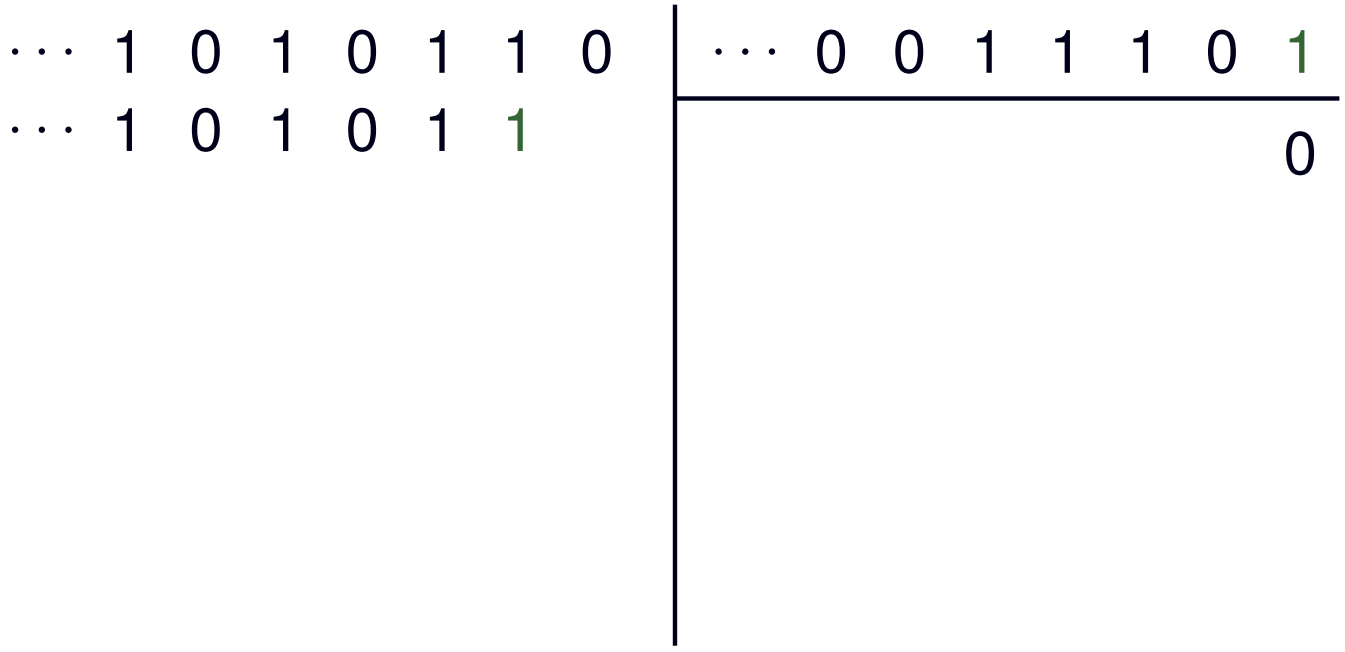
Structure de corps

Division



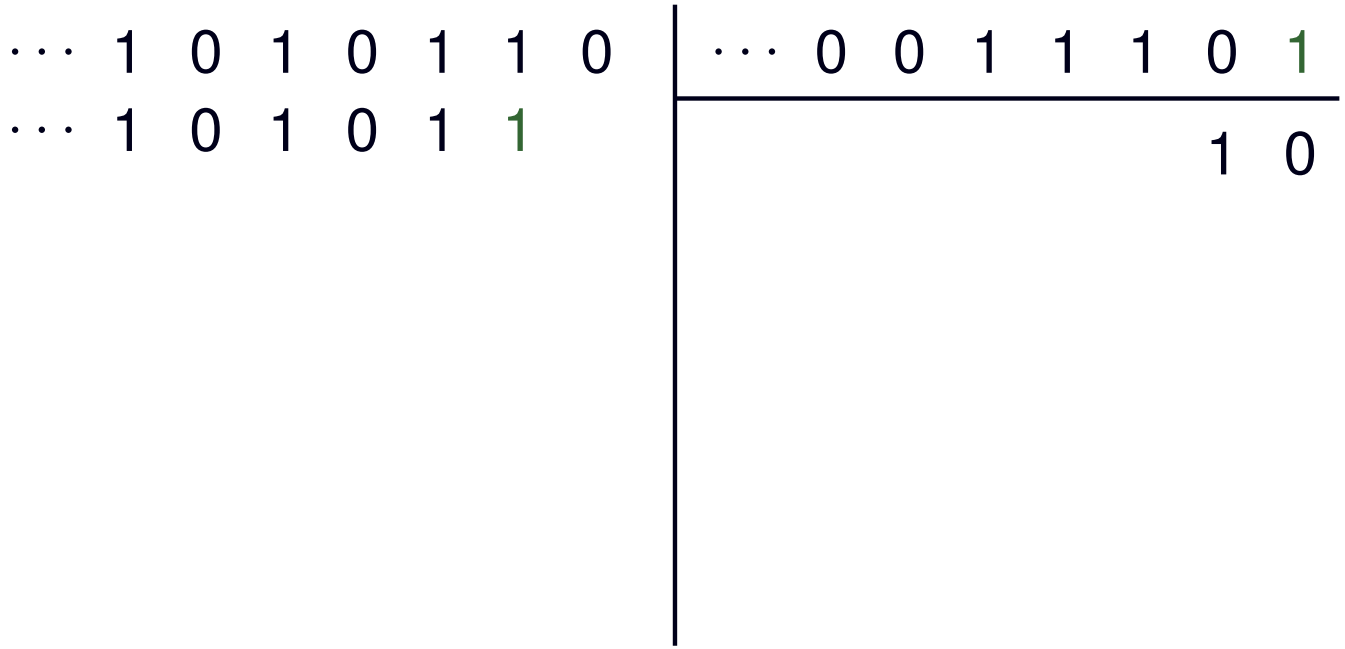
Structure de corps

Division



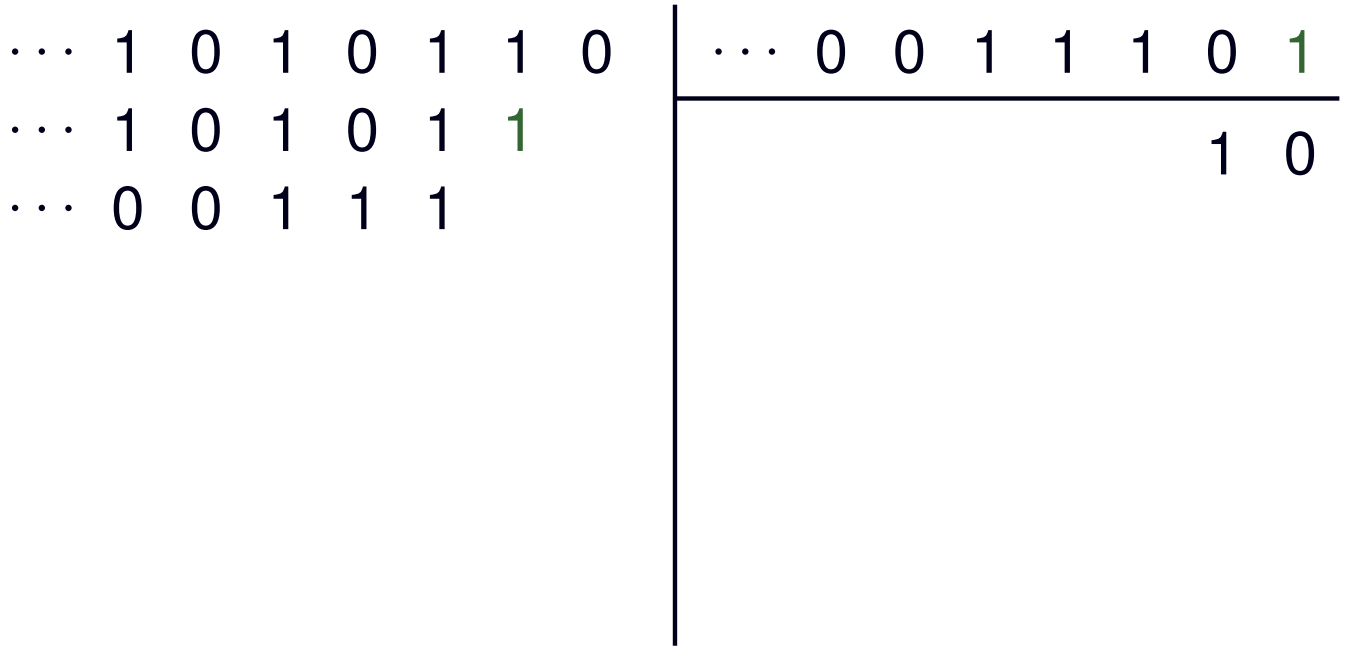
Structure de corps

Division



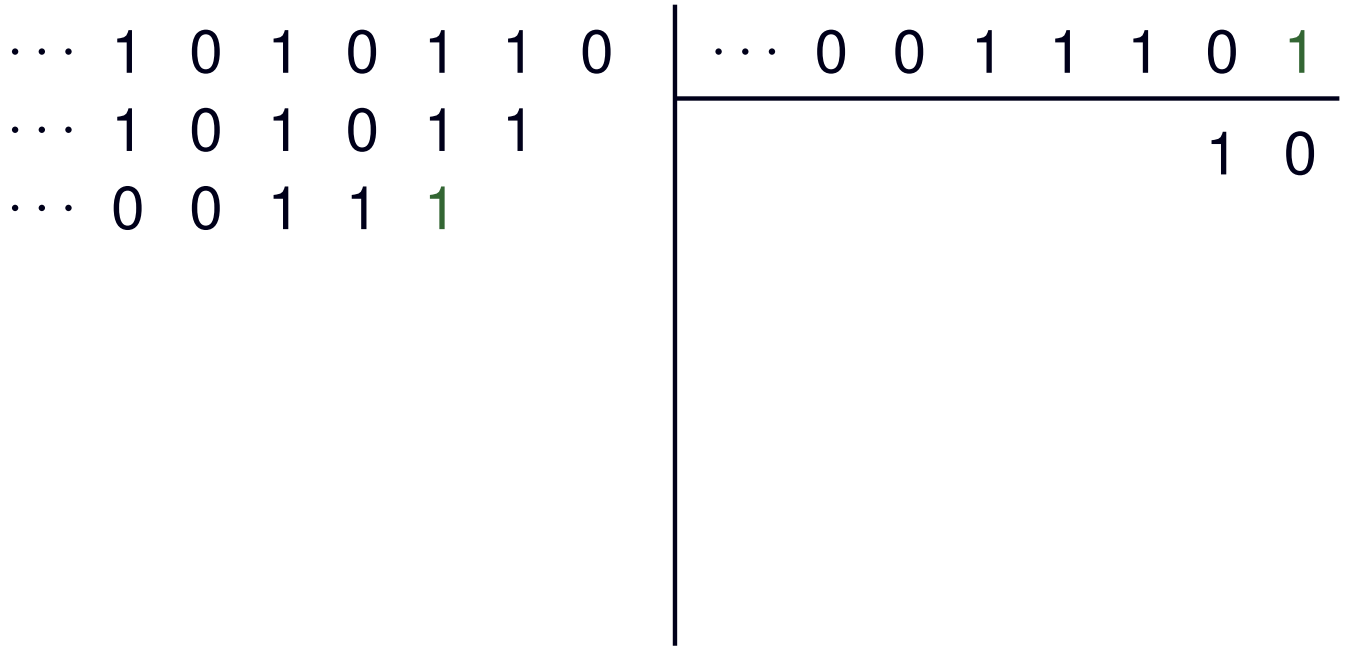
Structure de corps

Division



Structure de corps

Division



Structure de corps

Division

Structure de corps

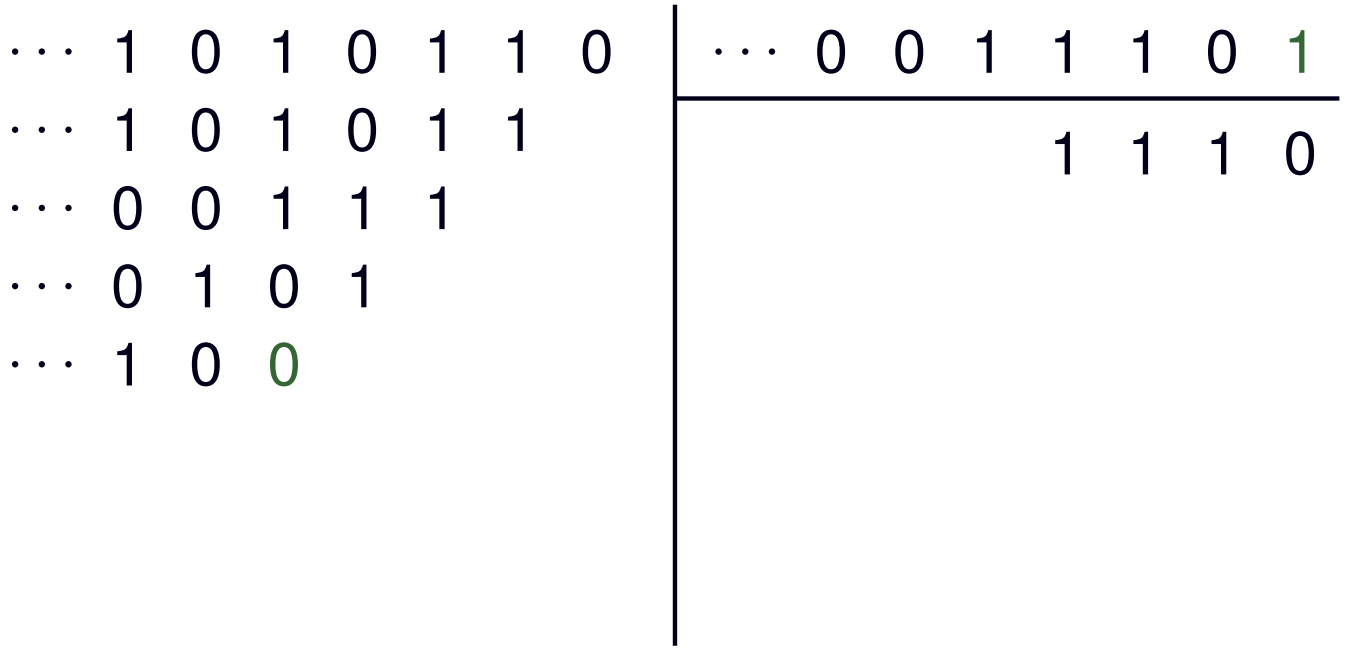
Division

Structure de corps

Division

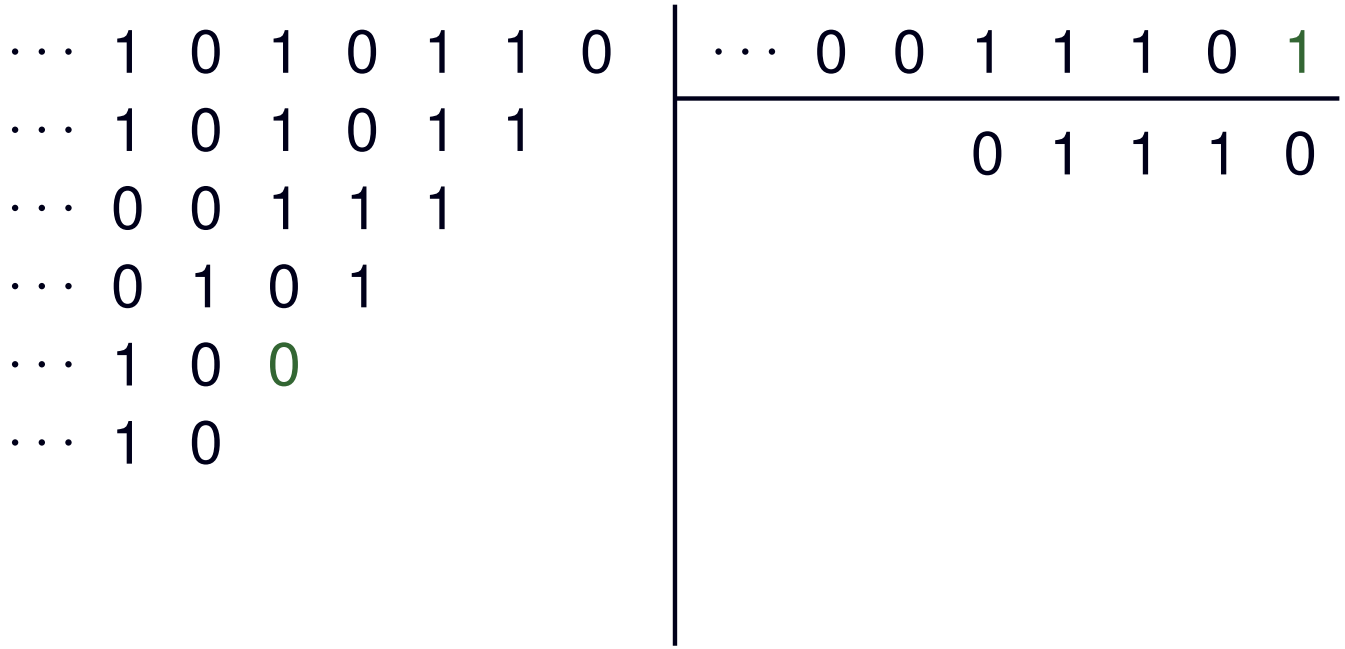
Structure de corps

Division



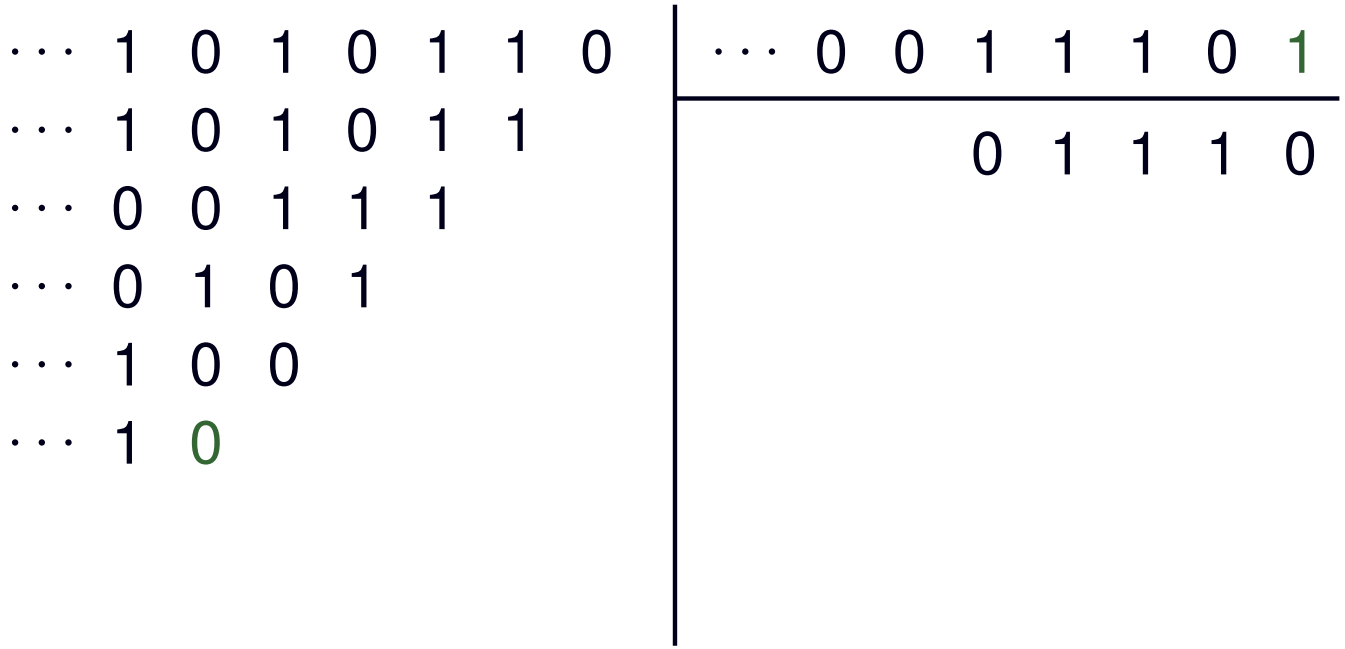
Structure de corps

Division



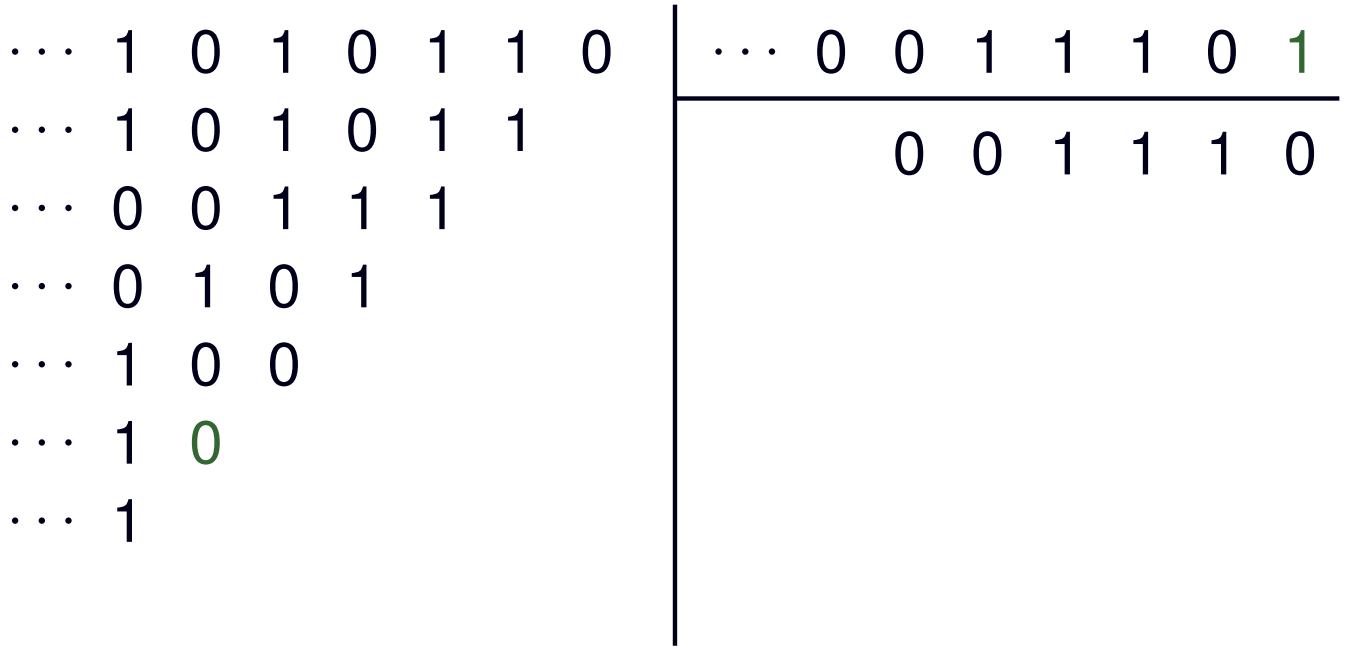
Structure de corps

Division



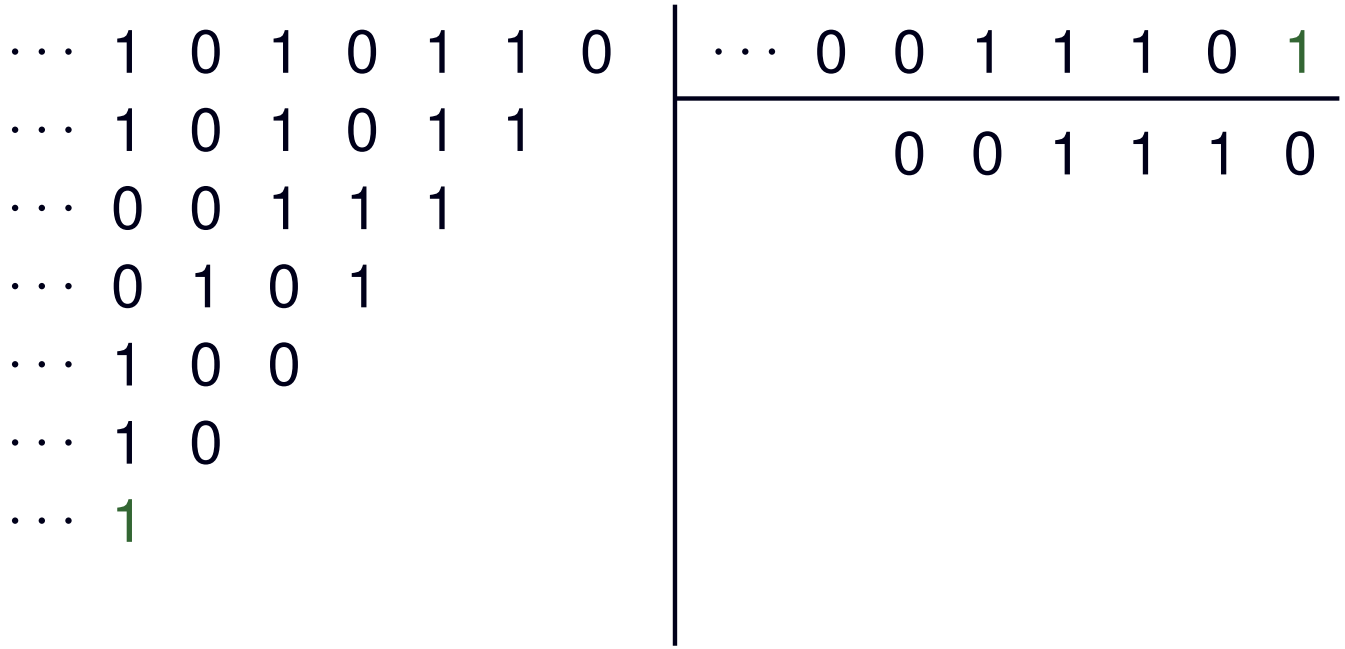
Structure de corps

Division



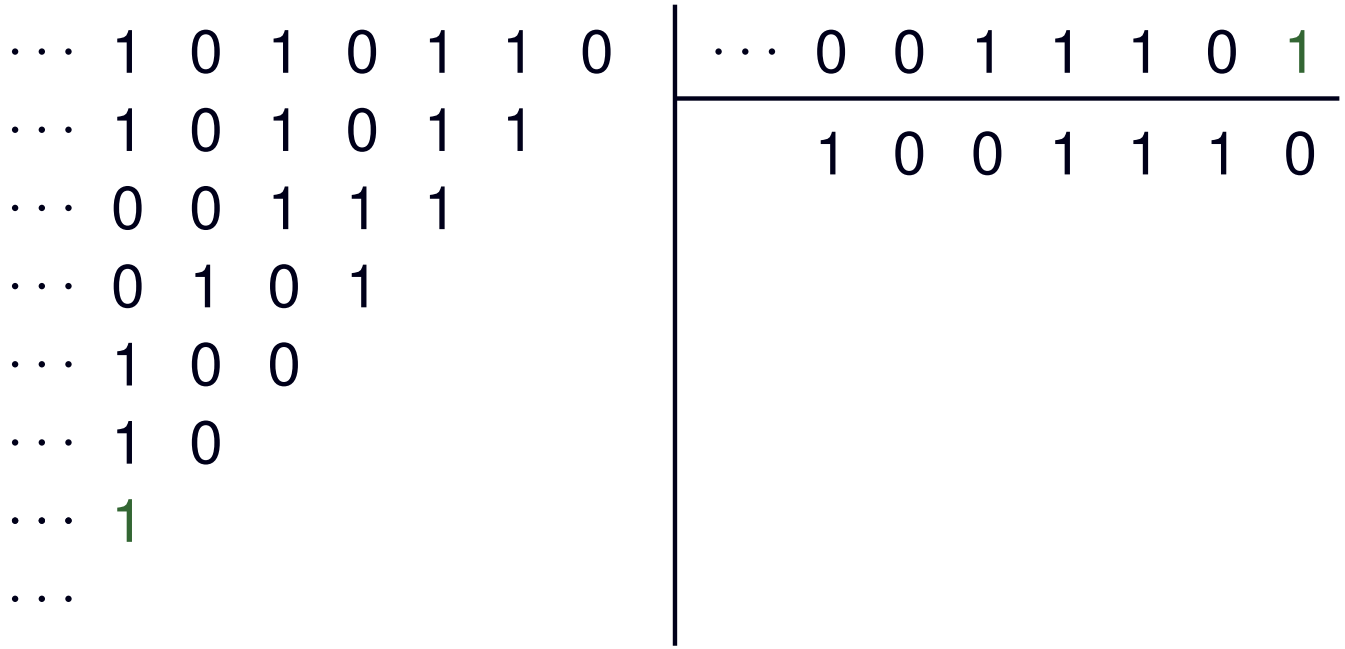
Structure de corps

Division



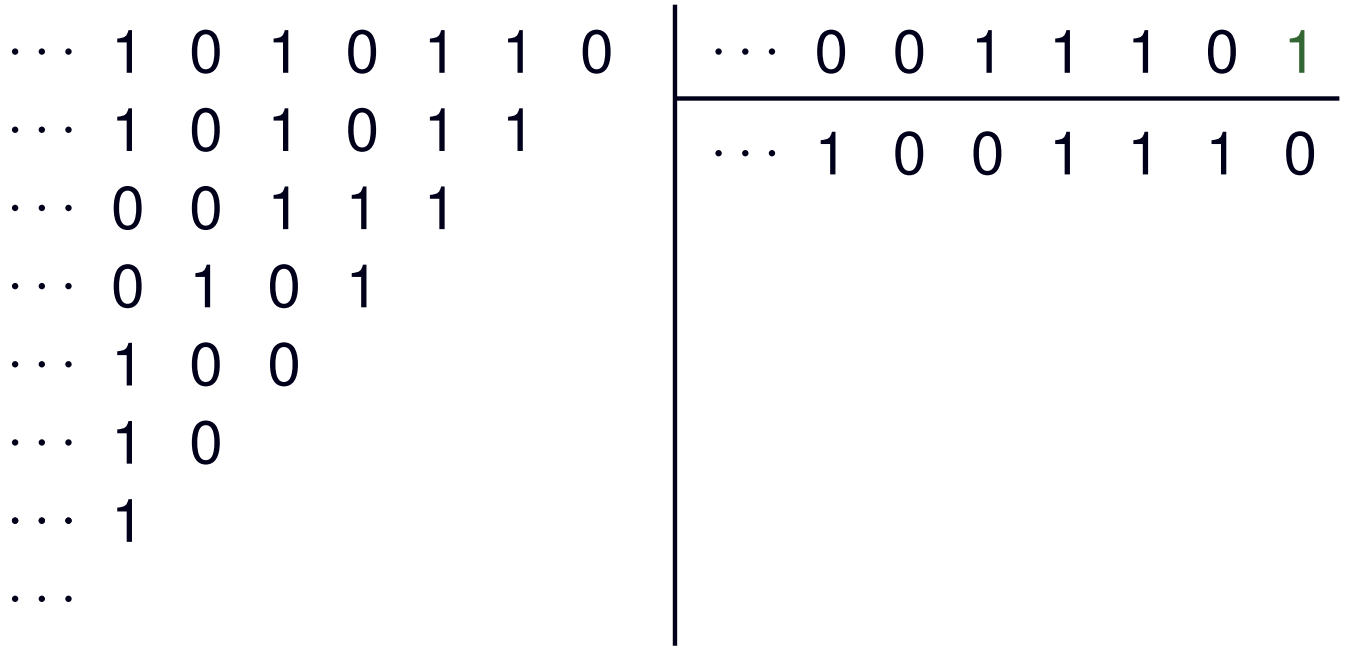
Structure de corps

Division



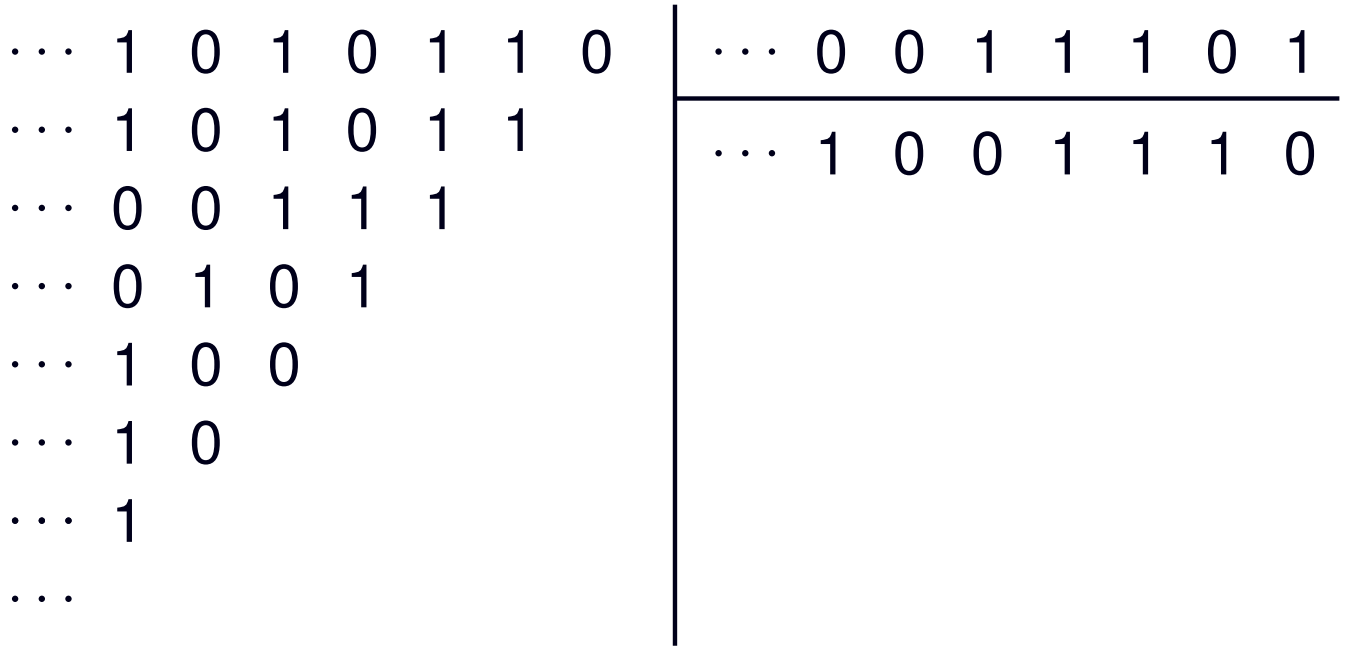
Structure de corps

Division



Structure de corps

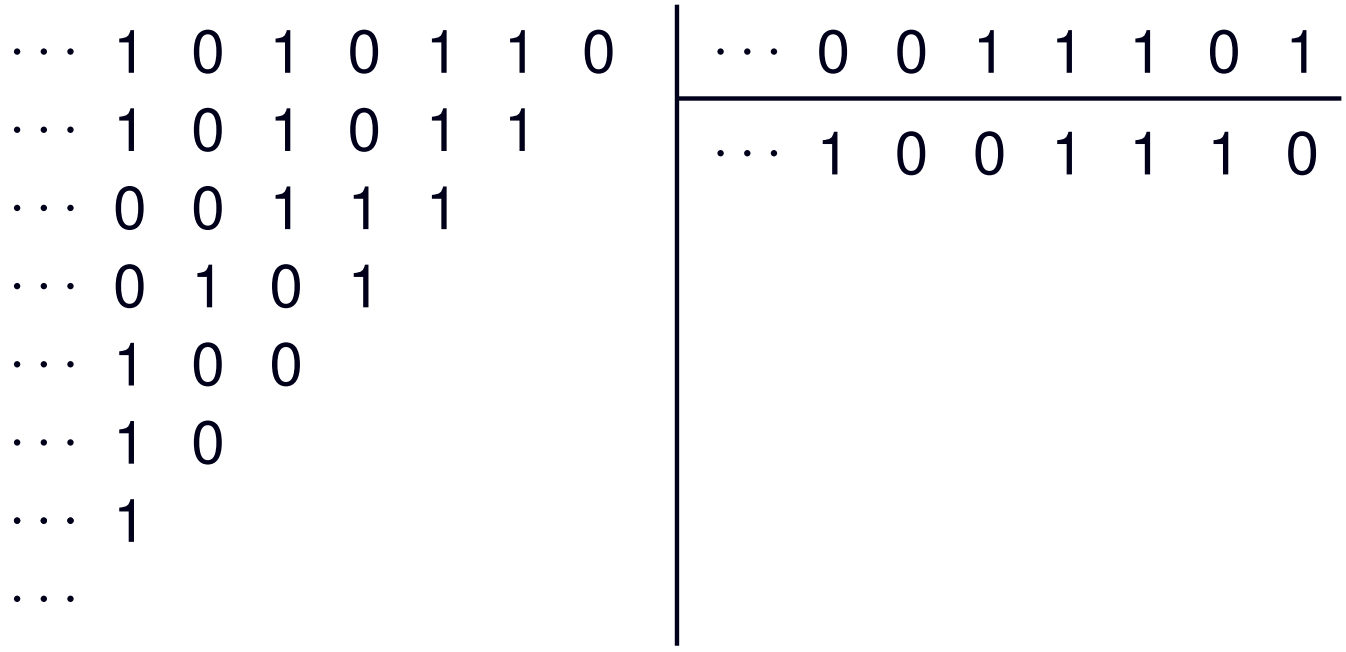
Division



Corollaire

Structure de corps

Division



Corollaire

$\mathbb{Z}_p$ est un anneau intègre local d'idéal maximal $p\mathbb{Z}_p$

Structure de corps

Division

$$
\begin{array}{llllllll|lllllll}
\cdots & 1 & 0 & 1 & 0 & 1 & 1 & 0 & \cdots & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\
\cdots & 1 & 0 & 1 & 0 & 1 & 1 & & \hline
\cdots & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\
\cdots & 0 & 0 & 1 & 1 & 1 & & & & & & & & & & \\
\cdots & 0 & 1 & 0 & 1 & & & & & & & & & & & \\
\cdots & 1 & 0 & 0 & & & & & & & & & & & & \\
\cdots & 1 & 0 & & & & & & & & & & & & & \\
\cdots & 1 & & & & & & & & & & & & & & \\
\cdots & & & & & & & & & & & & & & &
\end{array}
$$

Corollaire

$\mathbb{Z}_p$ est un anneau intègre local d'idéal maximal $p\mathbb{Z}_p$

$\mathbb{Q}_p = \mathbb{Z}_p[\frac{1}{p}] = \text{Frac } \mathbb{Z}_p$

Valuation et norme

Valuation et norme

Valuation p-adique

Valuation et norme

Valuation p-adique

$\mathrm{val}_p(x)$ est la positive du dernier chiffre non nul de x

Valuation et norme

Valuation p-adique

$\mathrm{val}_p(x)$ est la positive du dernier chiffre non nul de x

$$\mathrm{val}_p(\ldots 10110010) = 1$$

Valuation et norme

Valuation p-adique

$\mathrm{val}_p(x)$ est la positive du dernier chiffre non nul de x

$$\begin{aligned} \mathrm{val}_p(\ldots 10110010) &= 1 \\ \mathrm{val}_p(\ldots 10000010,001) &= -3 \end{aligned}$$

Valuation et norme

Valuation p-adique

$\mathrm{val}_p(x)$ est la positive du dernier chiffre non nul de x

$$\begin{aligned} \mathrm{val}_p(\ldots 10110010) &= 1 \\ \mathrm{val}_p(\ldots 10000010,001) &= -3 \\ \mathrm{val}_p(\ldots 00000000) &= ? \end{aligned}$$

Valuation et norme

Valuation p-adique

$\mathrm{val}_p(x)$ est la positive du dernier chiffre non nul de x

$$\begin{aligned} \mathrm{val}_p(\ldots 10110010) &= 1 \\ \mathrm{val}_p(\ldots 10000010,001) &= -3 \\ \mathrm{val}_p(\ldots 00000000) &\geq 8 \end{aligned}$$

Valuation et norme

Valuation p-adique

$\mathrm{val}_p(x)$ est la positive du dernier chiffre non nul de x

$$\begin{aligned} \mathrm{val}_p(\ldots 10110010) &= 1 \\ \mathrm{val}_p(\ldots 10000010,001) &= -3 \\ \mathrm{val}_p(\ldots 00000000) &\geq 8 \end{aligned}$$

Valeur absolue p-adique

Valuation et norme

Valuation p-adique

$\mathrm{val}_p(x)$ est la positive du dernier chiffre non nul de x

$$\begin{aligned} \mathrm{val}_p(\ldots 10110010) &= 1 \\ \mathrm{val}_p(\ldots 10000010,001) &= -3 \\ \mathrm{val}_p(\ldots 00000000) &\geq 8 \end{aligned}$$

Valeur absolue p-adique

$|x|_p = p^{-\mathrm{val}_p(x)}$

Valuation et norme

Valuation p-adique

$\mathrm{val}_p(x)$ est la positive du dernier chiffre non nul de x

$$\begin{aligned} \mathrm{val}_p(\ldots 10110010) &= 1 \\ \mathrm{val}_p(\ldots 10000010,001) &= -3 \\ \mathrm{val}_p(\ldots 00000000) &\geq 8 \end{aligned}$$

Valeur absolue p-adique

$$|x|_p = p^{-\mathrm{val}_p(x)}$$

$$|x+y|_p \leq \max\big(|x|_p, |y|_p\big)$$

Valuation et norme

Valuation p-adique

$\mathrm{val}_p(x)$ est la positive du dernier chiffre non nul de x

$$\begin{aligned} \mathrm{val}_p(\ldots 10110010) &= 1 \\ \mathrm{val}_p(\ldots 10000010,001) &= -3 \\ \mathrm{val}_p(\ldots 00000000) &\geq 8 \end{aligned}$$

Valeur absolue p-adique

$$|x|_p = p^{-\mathrm{val}_p(x)}$$

$$|x+y|_p \leq \max\big(|x|_p, |y|_p\big)$$

Résultats et observations

Valuation et norme

Valuation p-adique

$\mathrm{val}_p(x)$ est la positive du dernier chiffre non nul de x

$$\begin{aligned} \mathrm{val}_p(\ldots 10110010) &= 1 \\ \mathrm{val}_p(\ldots 10000010,001) &= -3 \\ \mathrm{val}_p(\ldots 00000000) &\geq 8 \end{aligned}$$

Valeur absolue p-adique

$|x|_p = p^{-\mathrm{val}_p(x)}$

$|x+y|_p \leq \max\big(|x|_p, |y|_p\big)$

Résultats et observations

$\mathbb{Q}_p$ est complet

Valuation et norme

Valuation p-adique

$\mathrm{val}_p(x)$ est la positive du dernier chiffre non nul de x

$$\begin{aligned} \mathrm{val}_p(\ldots 10110010) &= 1 \\ \mathrm{val}_p(\ldots 10000010,001) &= -3 \\ \mathrm{val}_p(\ldots 00000000) &\geq 8 \end{aligned}$$

Valeur absolue p-adique

$|x|_p = p^{-\mathrm{val}_p(x)}$

$|x+y|_p \leq \max\big(|x|_p, |y|_p\big)$

Résultats et observations

$\mathbb{Q}_p$ est complet, $\mathbb{Q}$ est dense dans $\mathbb{Q}_p$

Valuation et norme

Valuation p-adique

$\mathrm{val}_p(x)$ est la positive du dernier chiffre non nul de x

$$\begin{aligned} \mathrm{val}_p(\ldots 10110010) &= 1 \\ \mathrm{val}_p(\ldots 10000010,001) &= -3 \\ \mathrm{val}_p(\ldots 00000000) &\geq 8 \end{aligned}$$

Valeur absolue p-adique

$|x|_p = p^{-\mathrm{val}_p(x)}$

$|x+y|_p \leq \max\big(|x|_p, |y|_p\big)$

Résultats et observations

$\mathbb{Q}_p$ est complet, $\mathbb{Q}$ est dense dans $\mathbb{Q}_p$

$\mathbb{Z}_p = B_{\mathbb{Q}_p}(1)$

Valuation et norme

Valuation p-adique

$\mathrm{val}_p(x)$ est la positive du dernier chiffre non nul de x

$$\begin{aligned} \mathrm{val}_p(\ldots 10110010) &= 1 \\ \mathrm{val}_p(\ldots 10000010,001) &= -3 \\ \mathrm{val}_p(\ldots 00000000) &\geq 8 \end{aligned}$$

Valeur absolue p-adique

$|x|_p = p^{-\mathrm{val}_p(x)}$

$|x+y|_p \leq \max\big(|x|_p, |y|_p\big)$

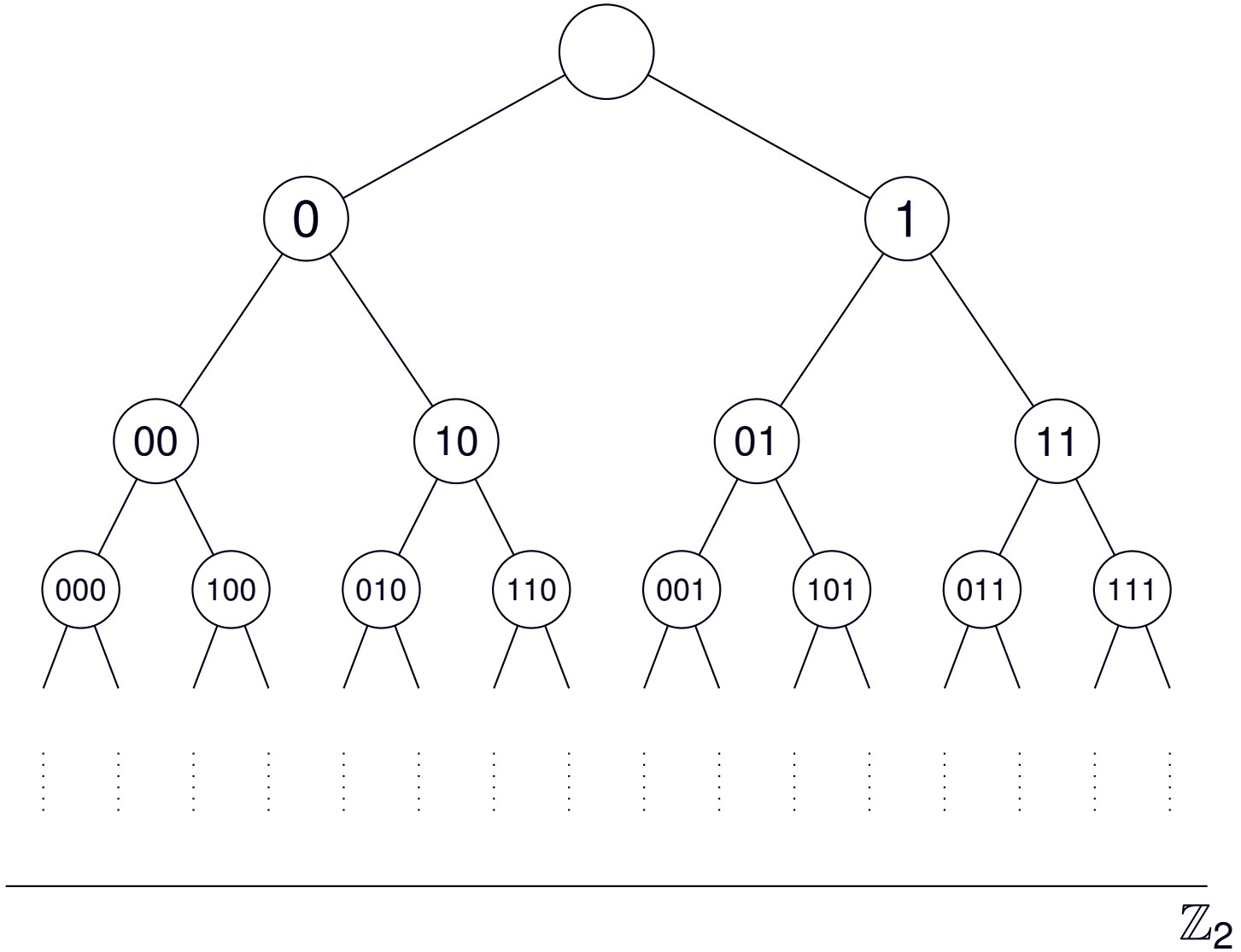
Résultats et observations

$\mathbb{Q}_p$ est complet, $\mathbb{Q}$ est dense dans $\mathbb{Q}_p$

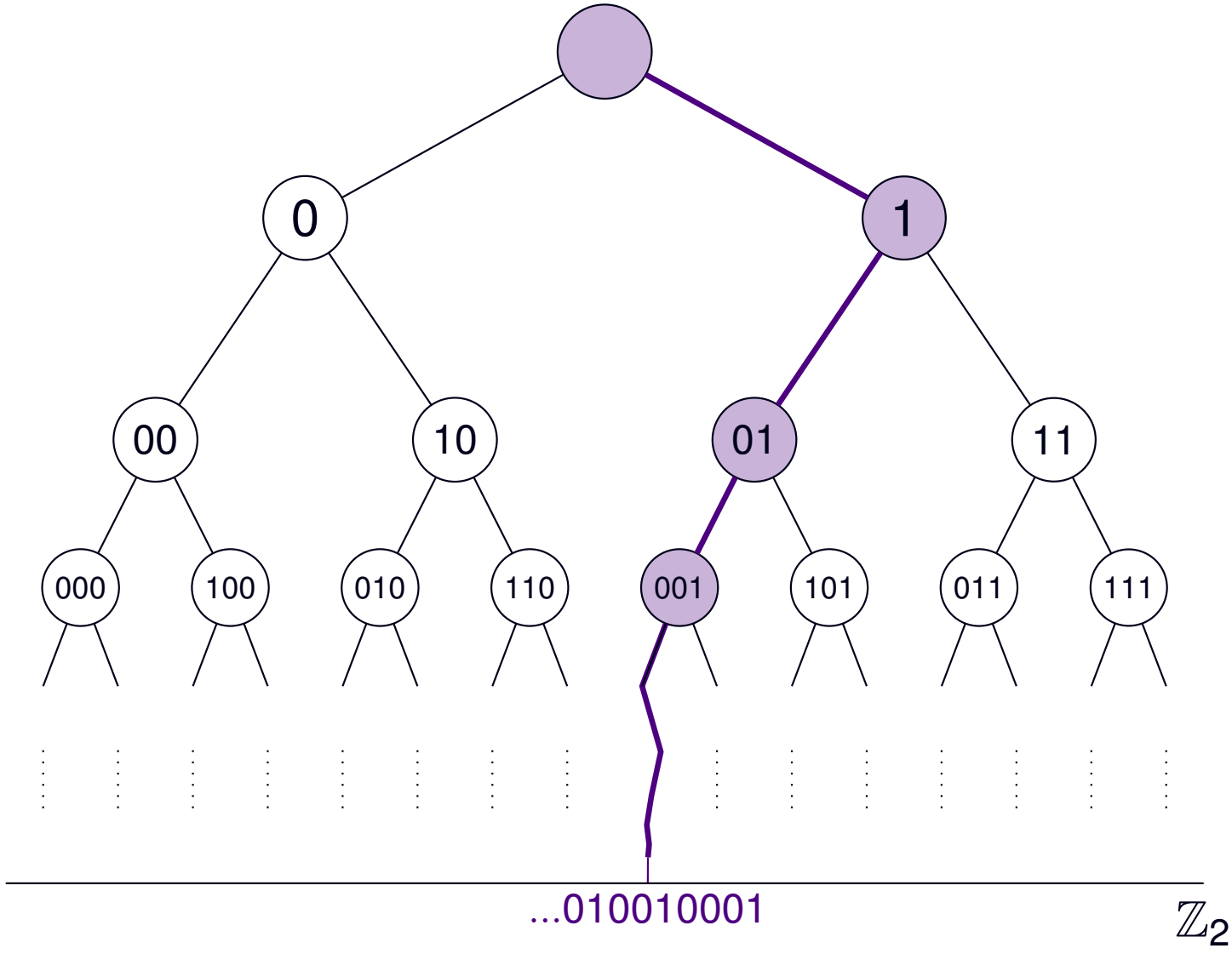
$\mathbb{Z}_p = B_{\mathbb{Q}_p}(1)$, $\mathbb{Z}_p^\times = \mathbb{S}_{\mathbb{Q}_p}(1)$

Représentation sous forme d’arbre

Représentation sous forme d'arbre



Représentation sous forme d'arbre

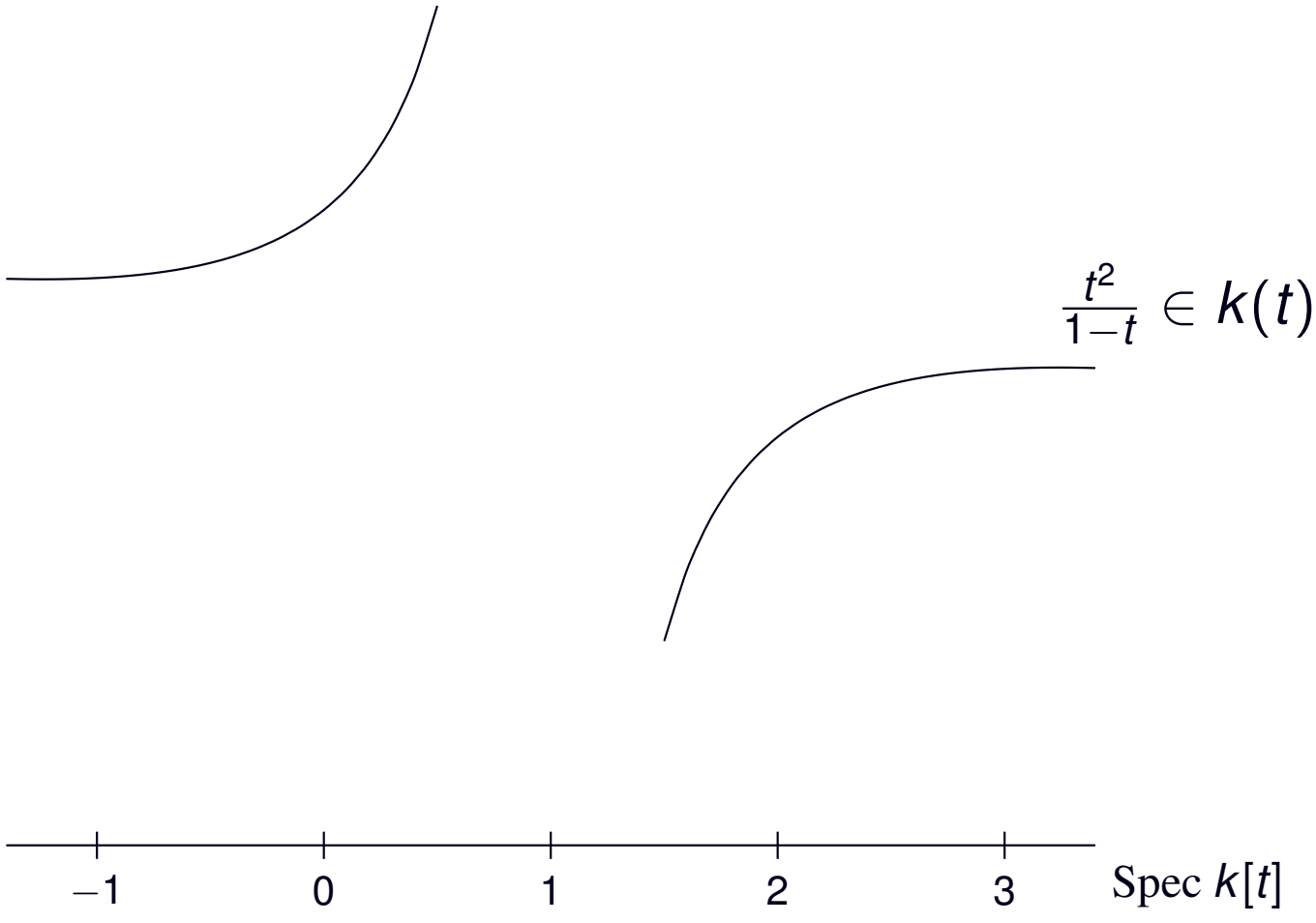


Le point de vue de la géométrie algébrique

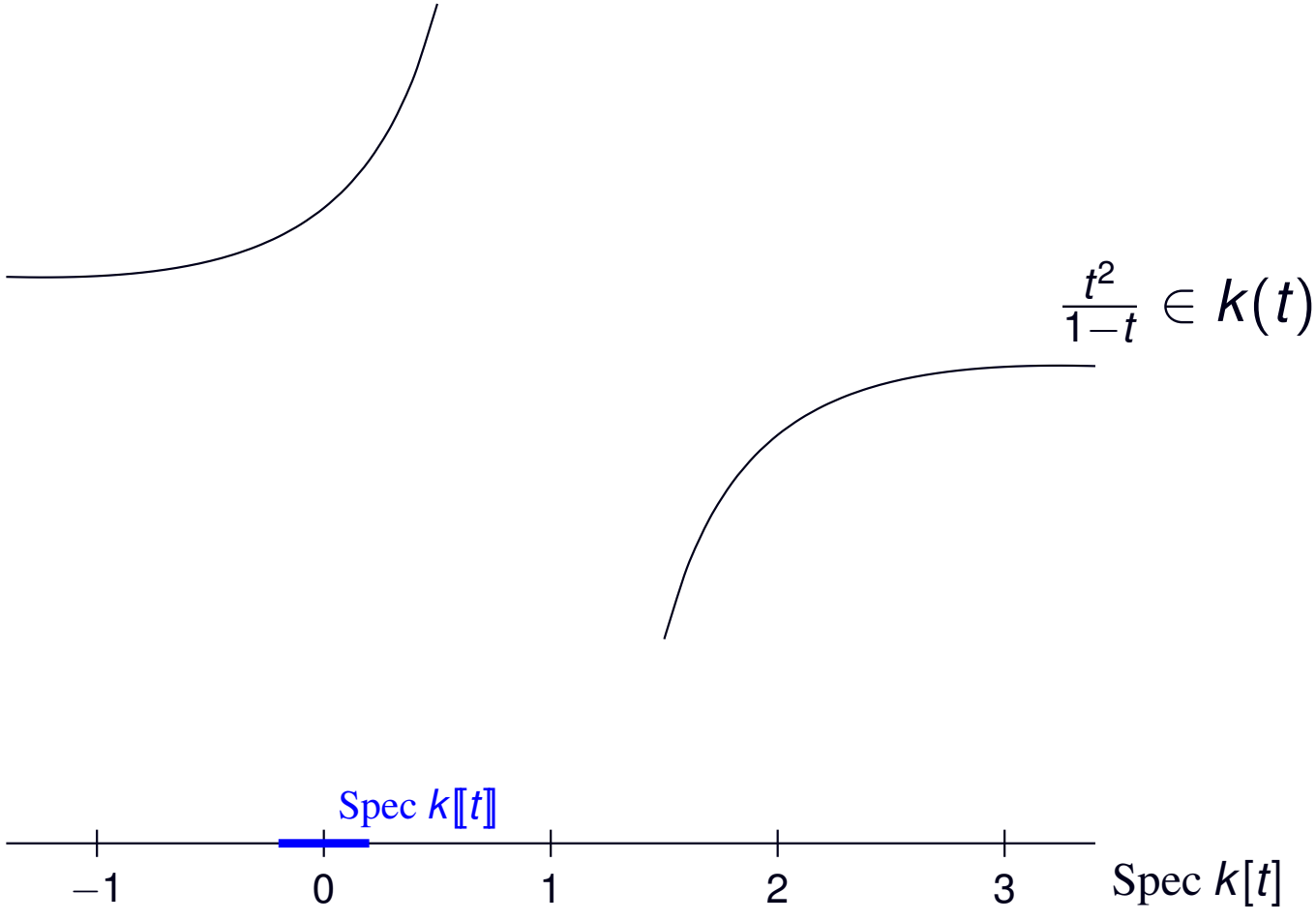
Le point de vue de la géométrie algébrique

Le point de vue de la géométrie algébrique

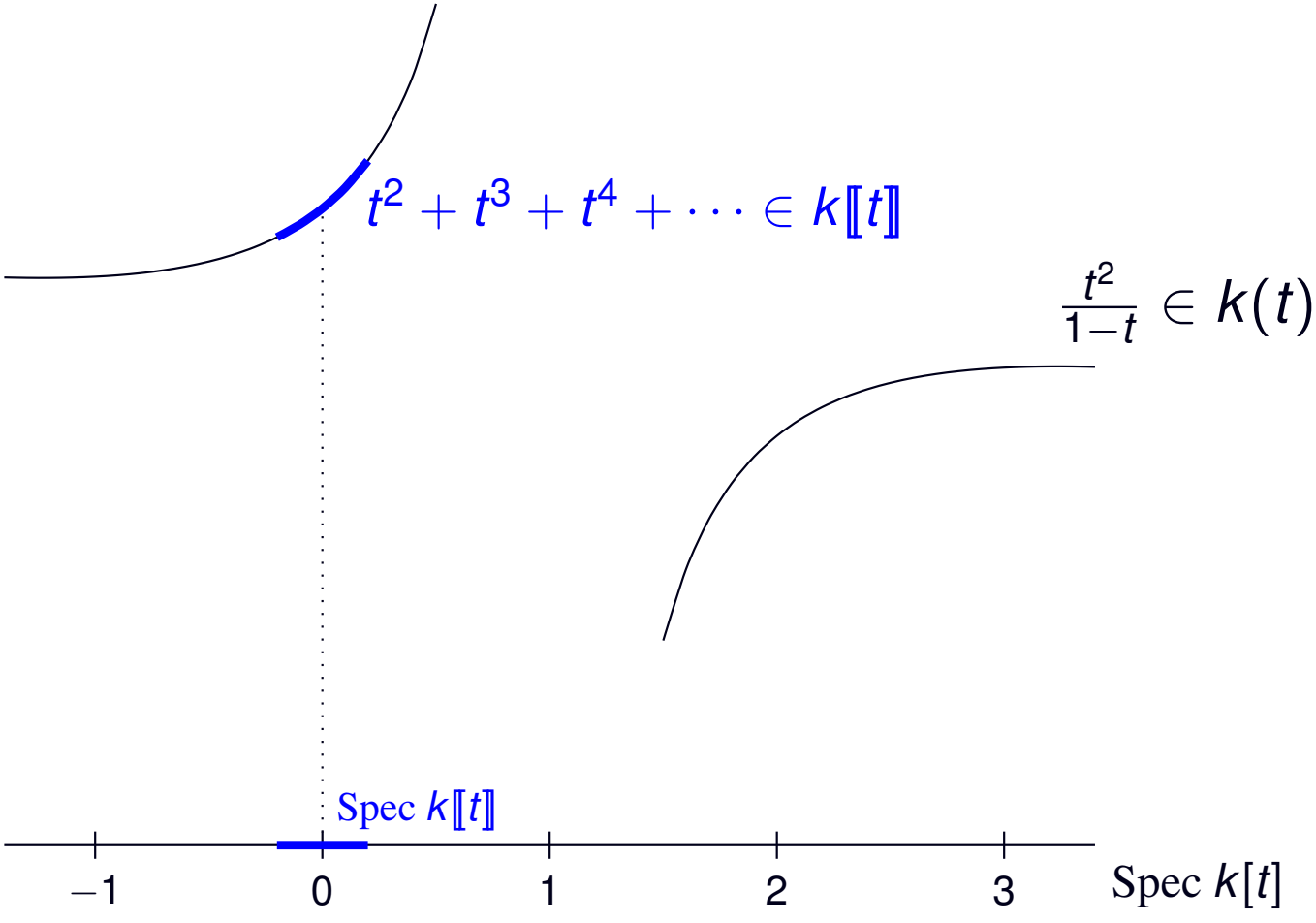
Le point de vue de la géométrie algébrique



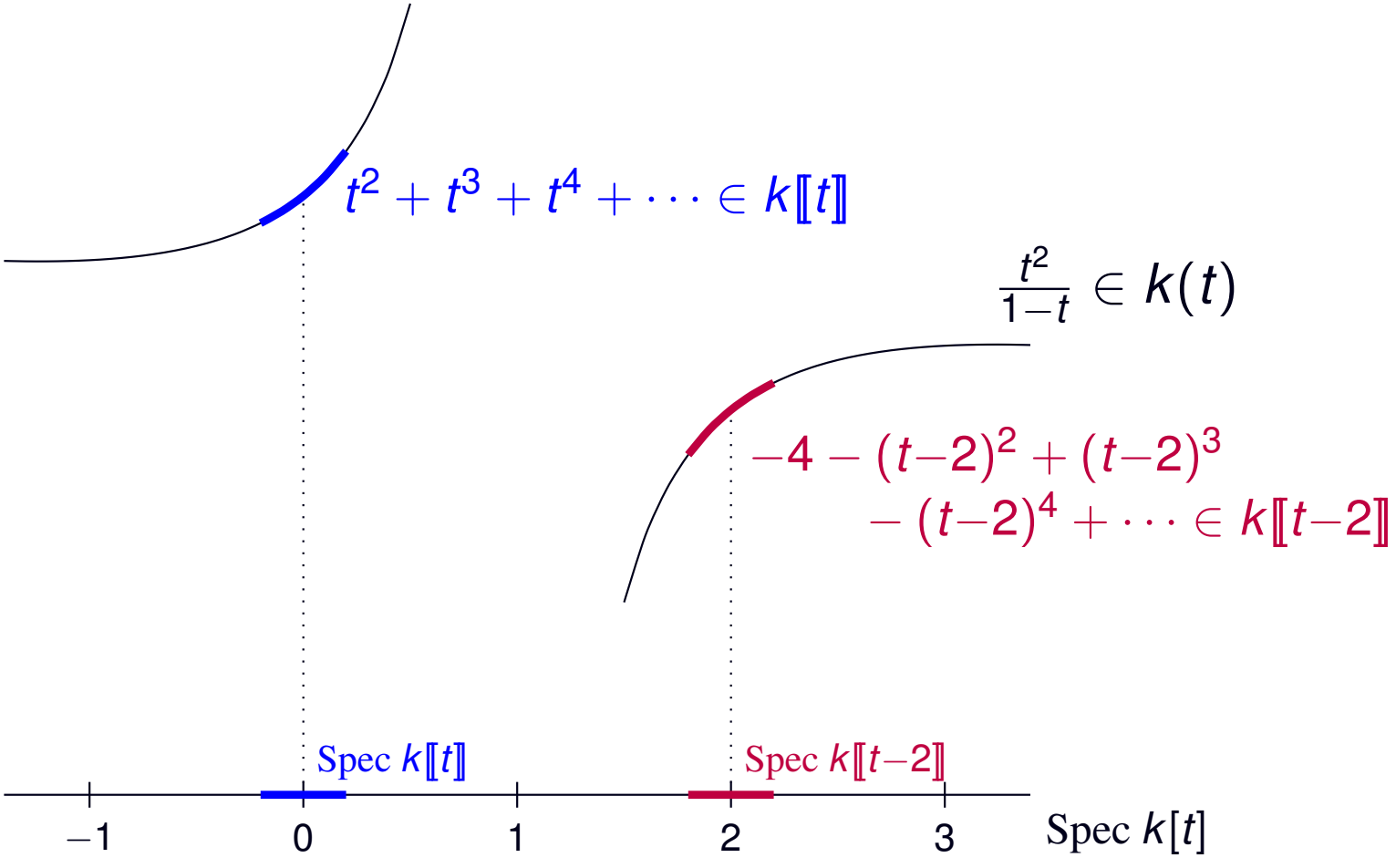
Le point de vue de la géométrie algébrique



Le point de vue de la géométrie algébrique



Le point de vue de la géométrie algébrique

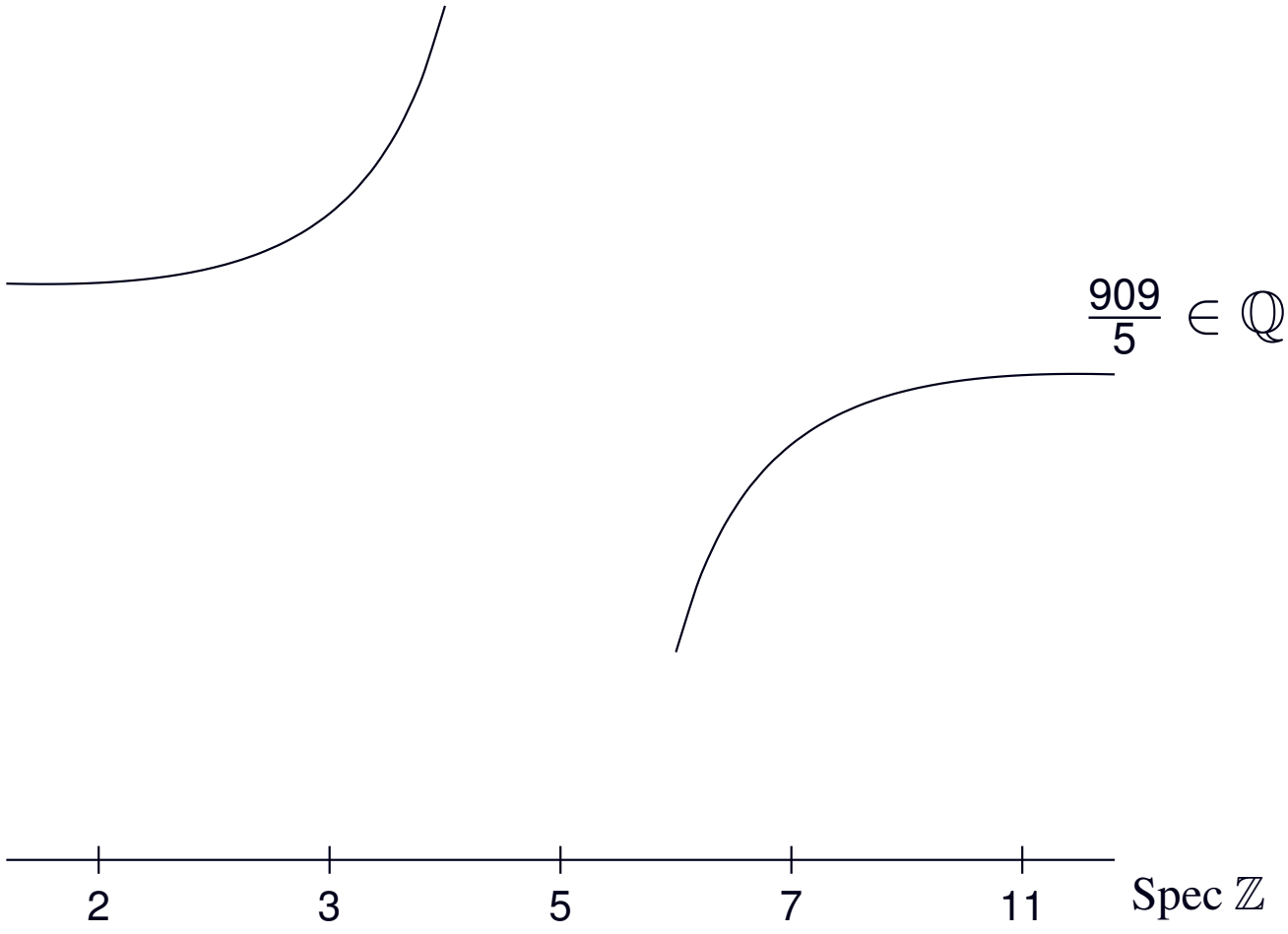


Le point de vue de la géométrie algébrique

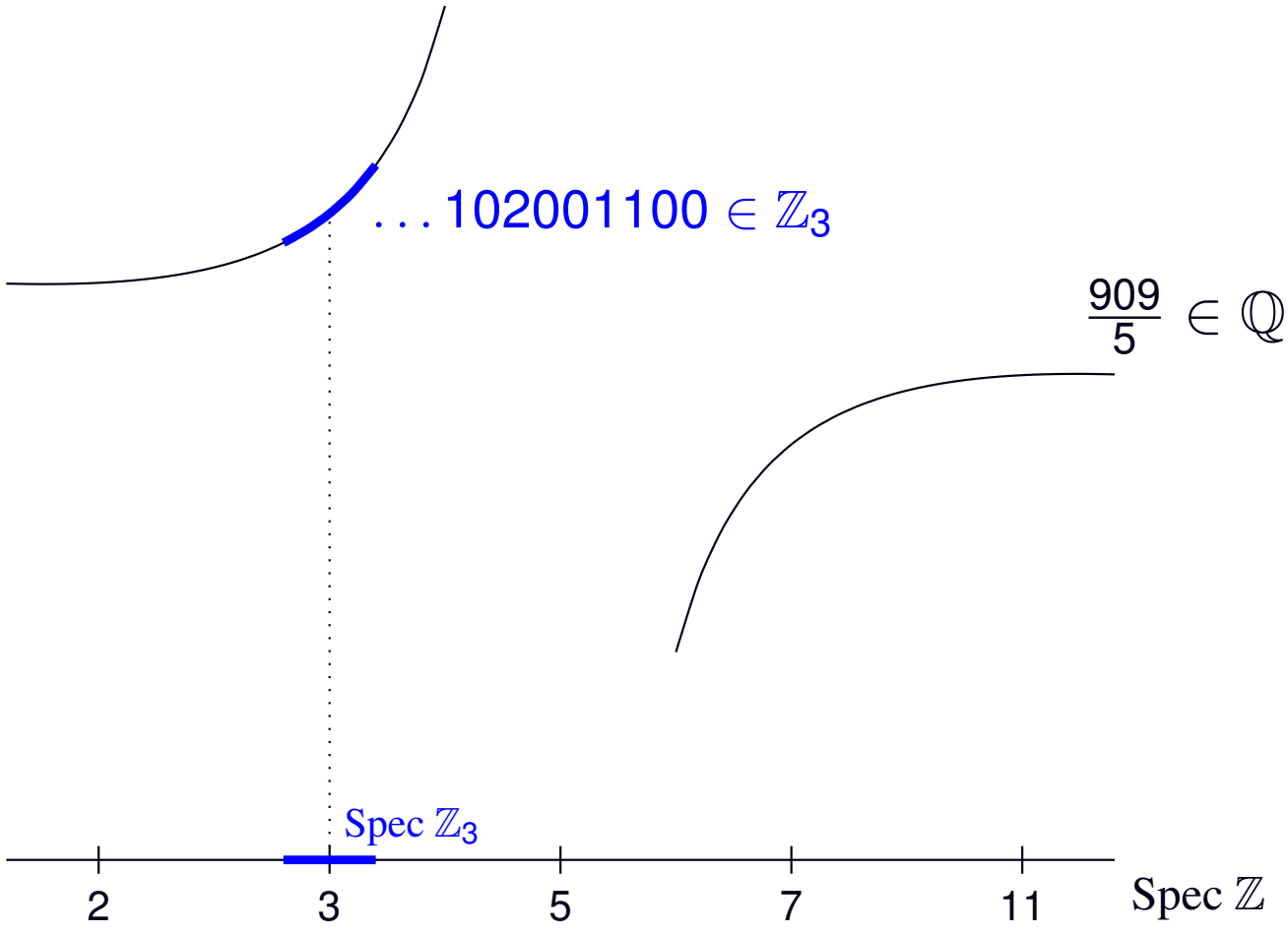
Le point de vue de la géométrie algébrique

Le point de vue de la géométrie algébrique

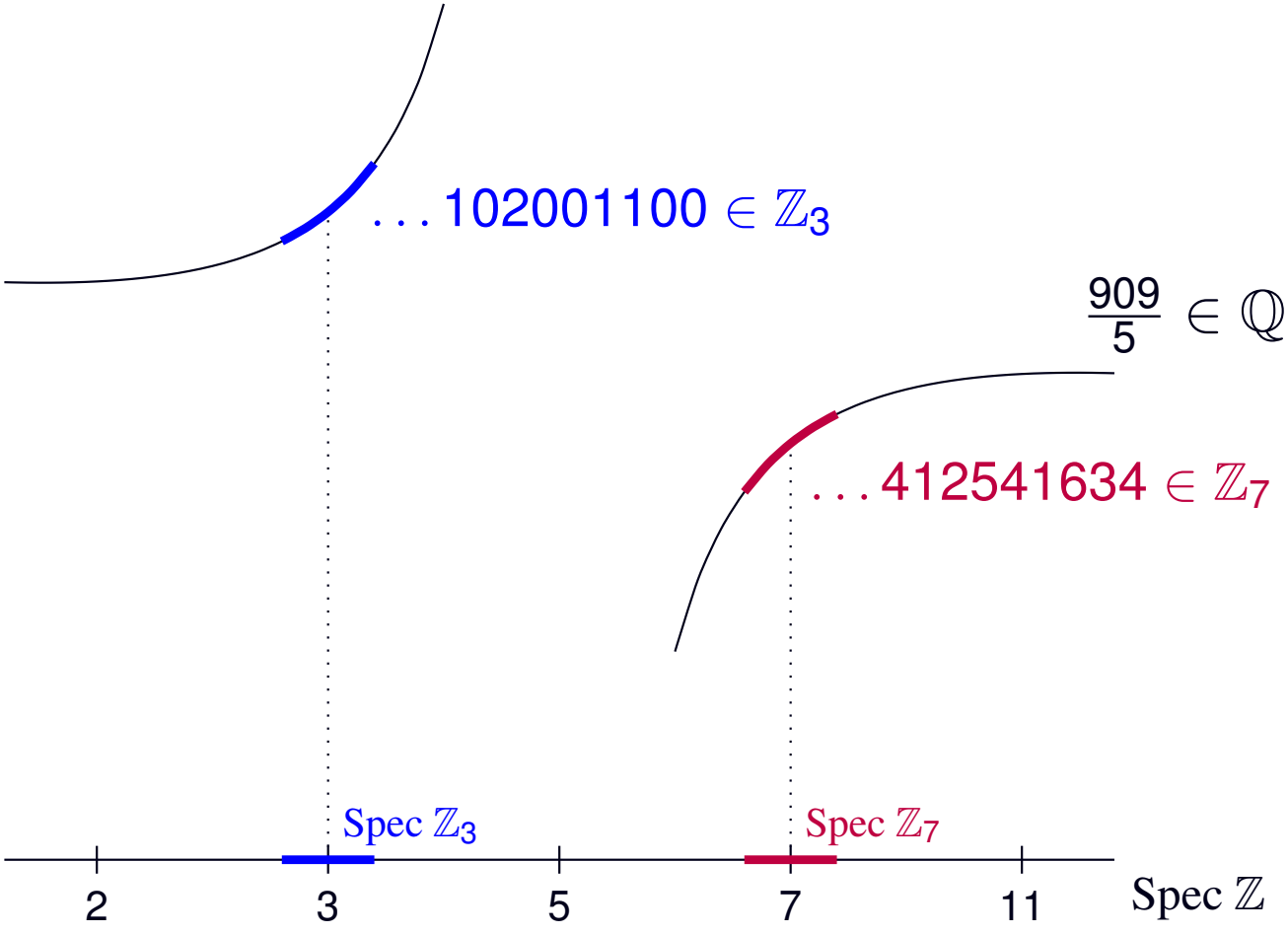
Le point de vue de la géométrie algébrique



Le point de vue de la géométrie algébrique

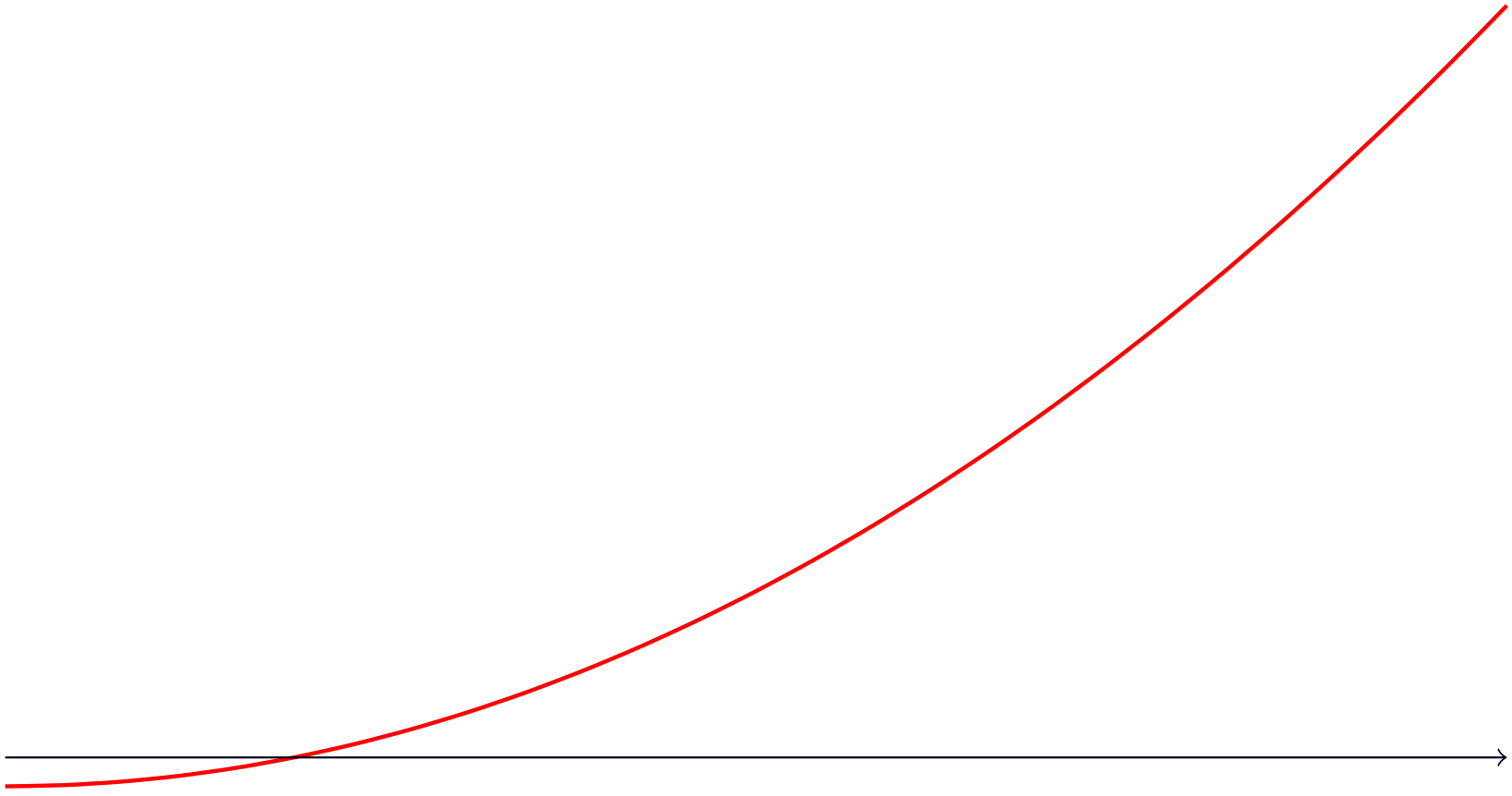


Le point de vue de la géométrie algébrique

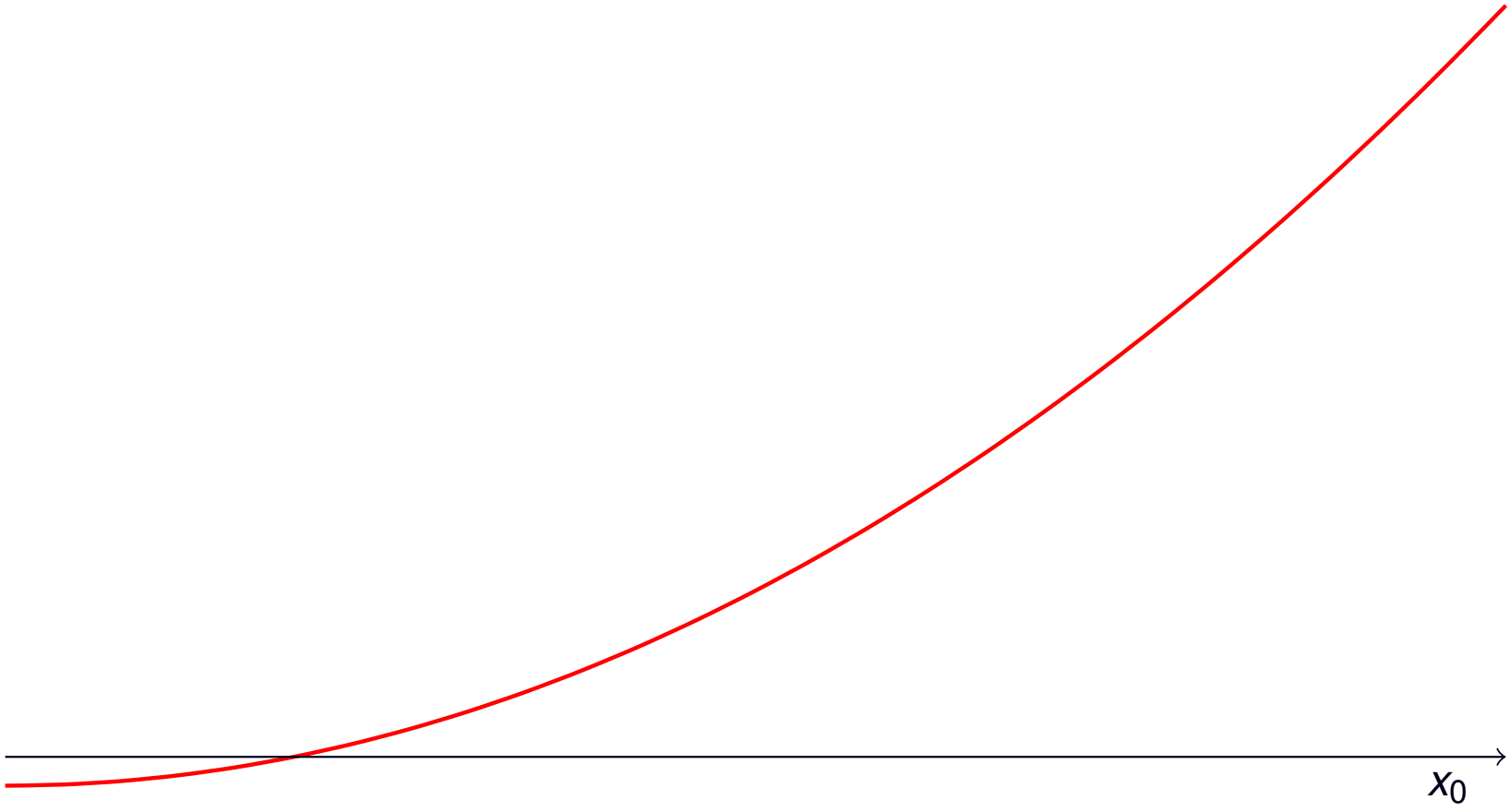


Itération de Newton

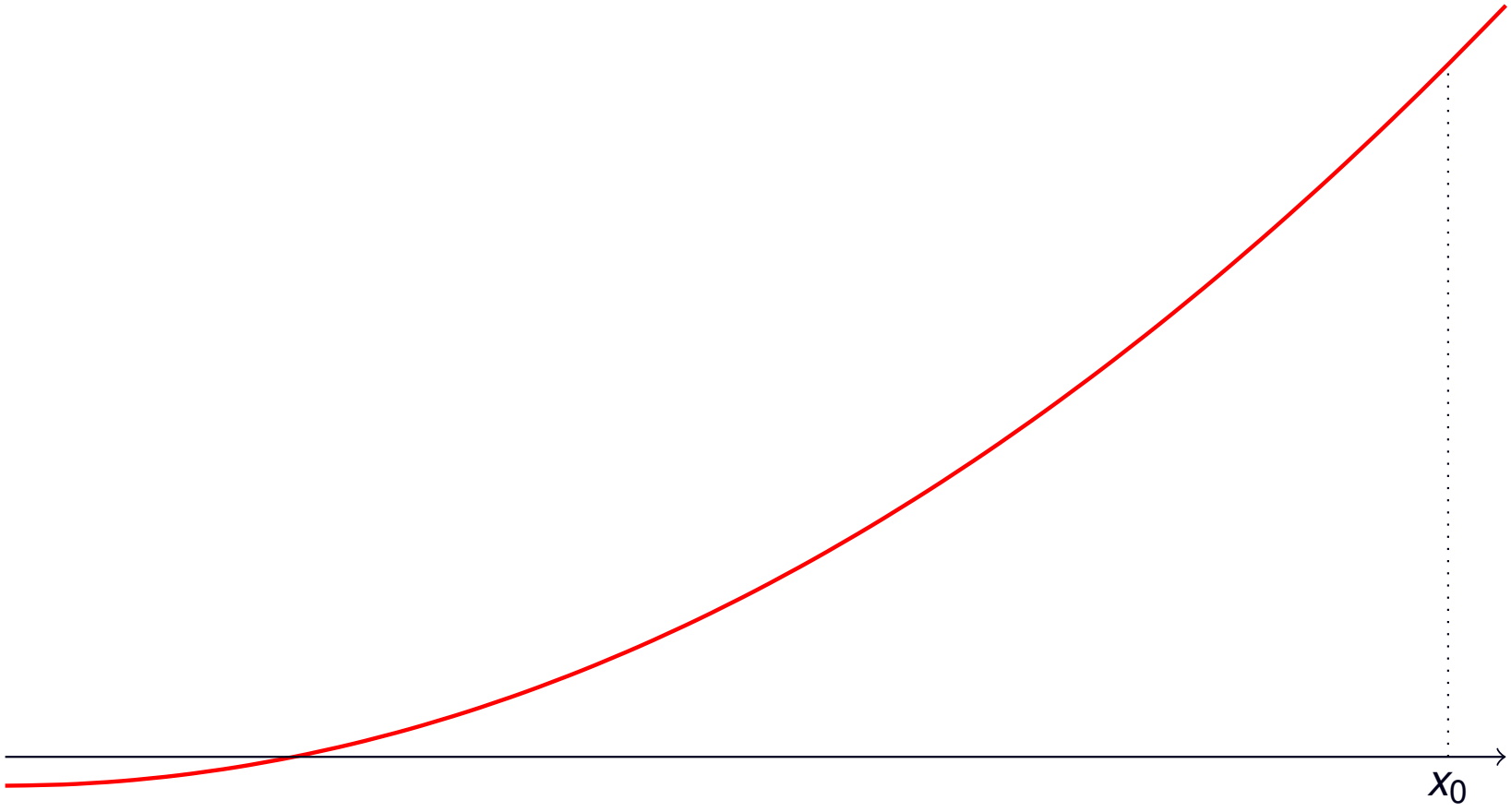
Itération de Newton



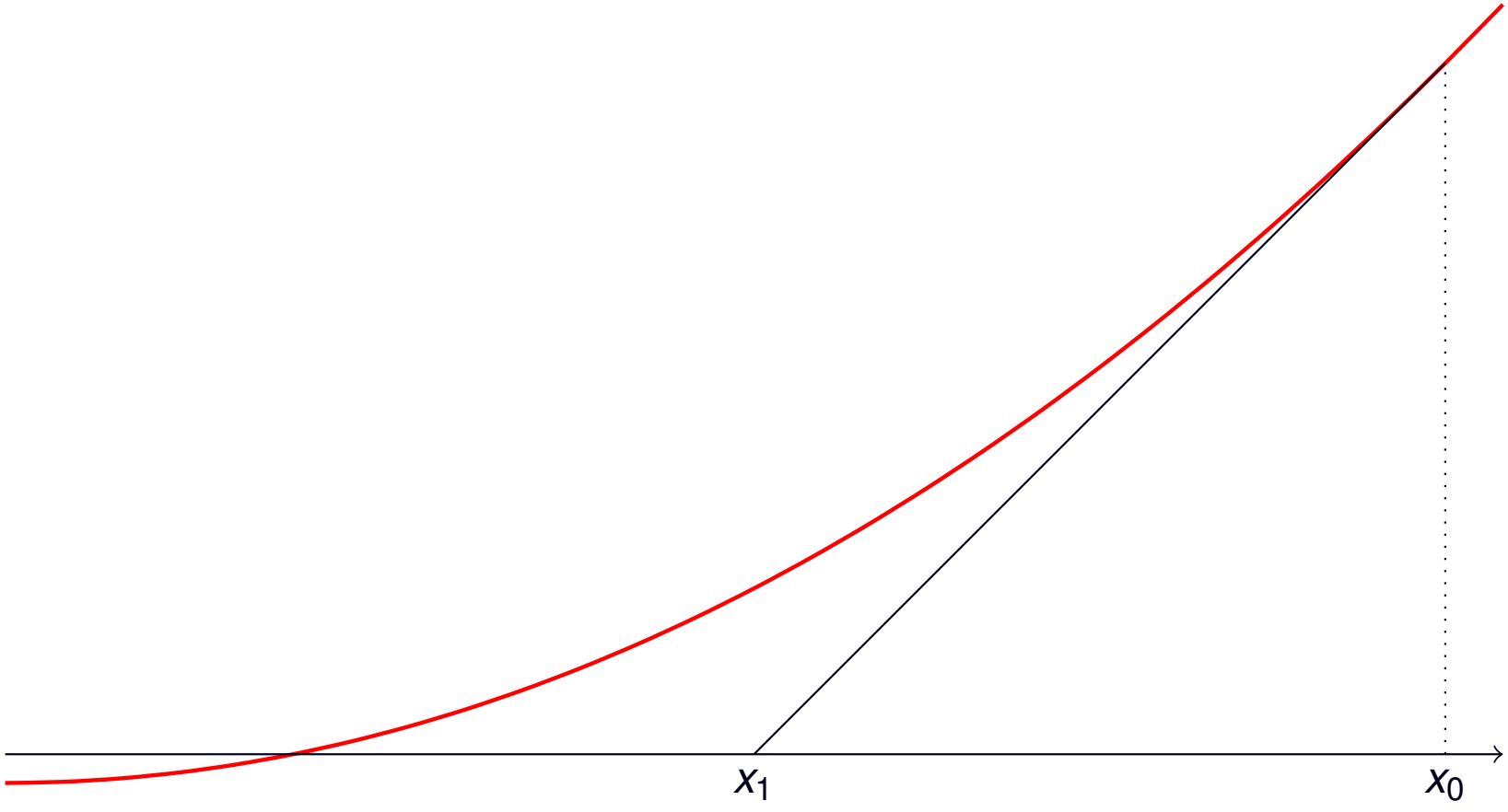
Itération de Newton



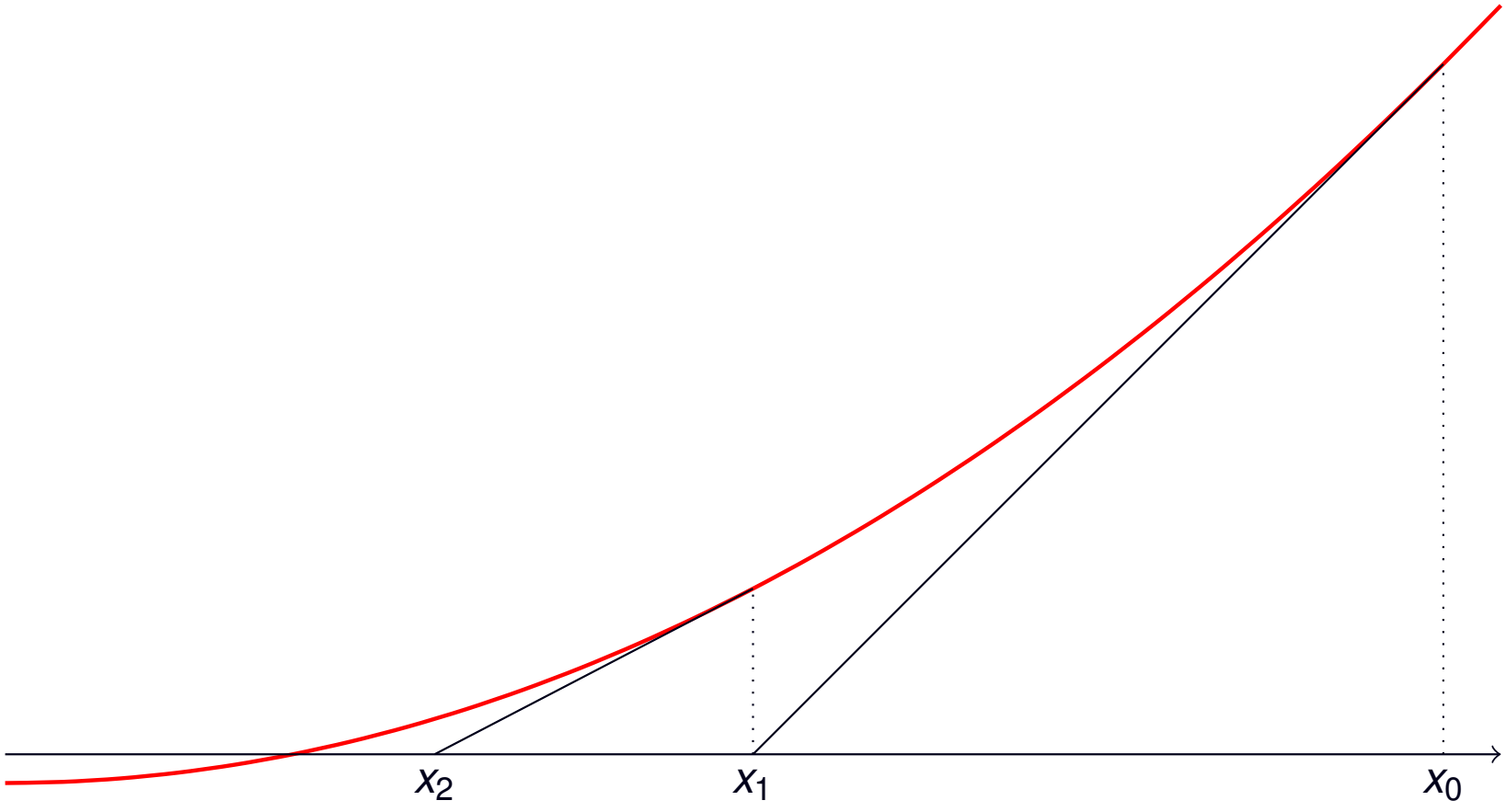
Itération de Newton



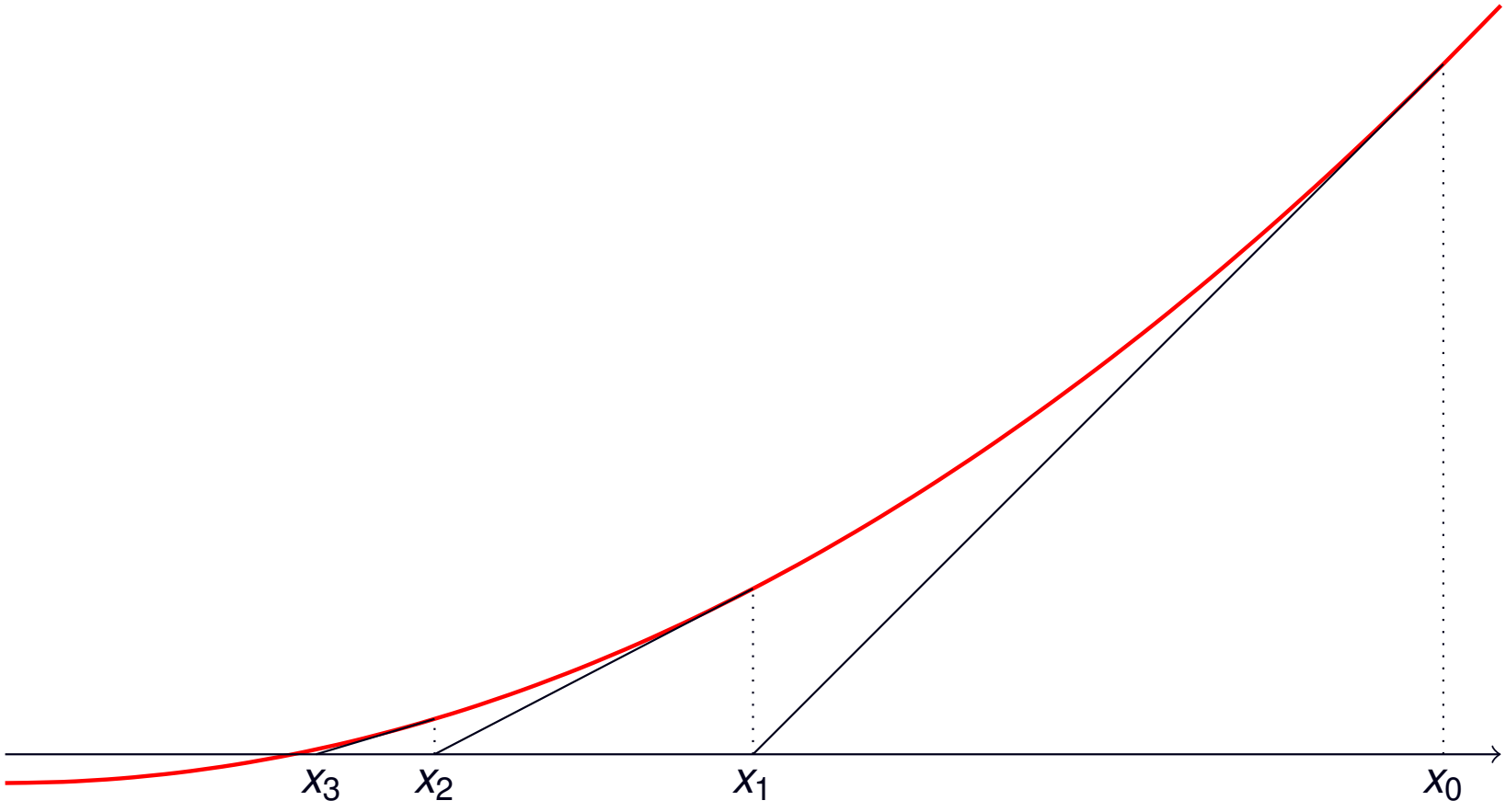
Itération de Newton



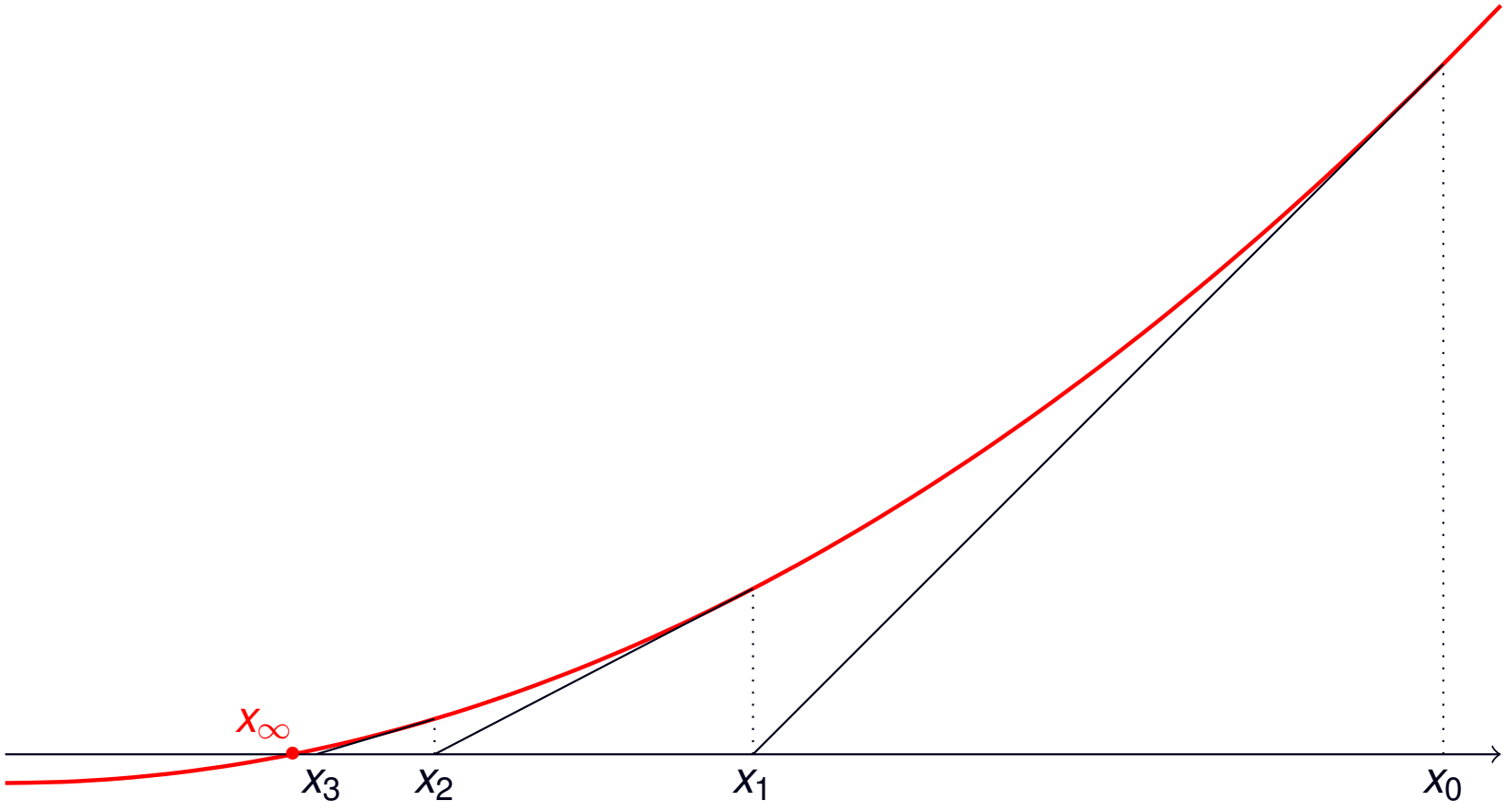
Itération de Newton



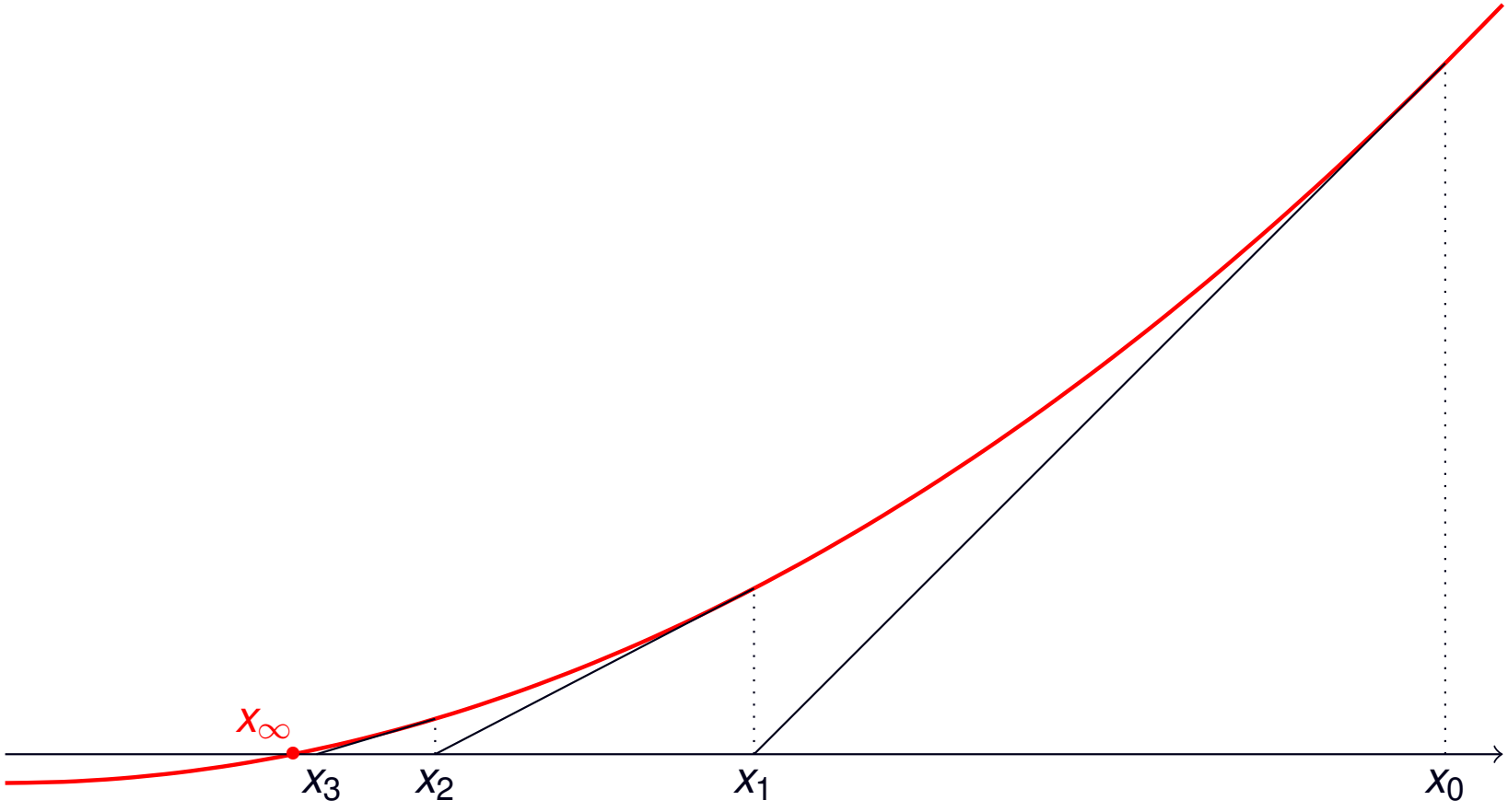
Itération de Newton



Itération de Newton



Itération de Newton



$$x_{i+1} = x_i - \frac{f(x_i)}{f'(x_i)}$$

Itération de Newton

Itération de Newton

Lemme de Hensel

Itération de Newton

Lemme de Hensel

Soit $f : \mathbb{Z}_p \to \mathbb{Q}_p$ une fonction de classe C^2.

Itération de Newton

Lemme de Hensel

Soit $f : \mathbb{Z}_p \to \mathbb{Q}_p$ une fonction de classe C^2.

Soit $a \in \mathbb{Z}_p$ tel que :

$$|f(a)| < \frac{|f'(a)|^2}{\|f''\|_\infty} \quad \text{et} \quad |f(a)| < |f'(a)|.$$

Itération de Newton

Lemme de Hensel

Soit $f : \mathbb{Z}_p \to \mathbb{Q}_p$ une fonction de classe C^2.

Soit $a \in \mathbb{Z}_p$ tel que :

$$|f(a)| < \frac{|f'(a)|^2}{\|f''\|_\infty} \quad \text{et} \quad |f(a)| < |f'(a)|.$$

Alors, la suite récurrente définie par

$$x_0 = a \quad ; \quad x_{i+1} = x_i - \frac{f(x_i)}{f'(x_i)}$$

converge vers un zéro de f.

Itération de Newton

Lemme de Hensel

Soit $f : \mathbb{Z}_p \to \mathbb{Q}_p$ une fonction de classe C^2.

Soit $a \in \mathbb{Z}_p$ tel que :

$$|f(a)| < \frac{|f'(a)|^2}{\|f''\|_\infty} \quad \text{et} \quad |f(a)| < |f'(a)|.$$

Alors, la suite récurrente définie par

$$x_0 = a \quad ; \quad x_{i+1} = x_i - \frac{f(x_i)}{f'(x_i)}$$

converge vers un zéro de f.

C'est le seul dans la boule de centre a et de rayon $\dfrac{|f'(a)|}{\|f''\|_\infty}$.

Itération de Newton

Itération de Newton

Calcul de c^{-1}

Itération de Newton

Calcul de c^{-1} pour $c \in \mathbb{Z}_p^\times$

Itération de Newton

Calcul de c^{-1} pour $c \in \mathbb{Z}_p^\times$

$$f(x) = \frac{1}{x} - c$$

Itération de Newton

Calcul de c^{-1} pour $c \in \mathbb{Z}_p^\times$

$$f(x) = \frac{1}{x} - c \quad ; \quad f'(x) = -\frac{1}{x^2}$$

Itération de Newton

Calcul de c^{-1} pour $c \in \mathbb{Z}_p^\times$

$$f(x) = \frac{1}{x} - c \quad ; \quad f'(x) = -\frac{1}{x^2}$$

$$x_0 = c^{-1} \bmod p$$

Itération de Newton

Calcul de c^{-1} pour $c \in \mathbb{Z}_p^\times$

$$f(x) = \frac{1}{x} - c \quad ; \quad f'(x) = -\frac{1}{x^2}$$

$$x_0 = c^{-1} \bmod p \quad ; \quad x_{i+1} = 2x_i - cx_i^2$$

Itération de Newton

Calcul de c^{-1} pour $c \in \mathbb{Z}_p^\times$

$$f(x) = \frac{1}{x} - c \quad ; \quad f'(x) = -\frac{1}{x^2}$$

$$x_0 = c^{-1} \bmod p \quad ; \quad x_{i+1} = 2x_i - cx_i^2$$

$$\left[\, cx_{i+1} - 1 = -(cx_i - 1)^2 \,\right]$$

Itération de Newton

Calcul de c^{-1} pour $c \in \mathbb{Z}_p^\times$

$$f(x) = \frac{1}{x} - c \quad ; \quad f'(x) = -\frac{1}{x^2}$$

$$x_0 = c^{-1} \bmod p \quad ; \quad x_{i+1} = 2x_i - cx_i^2$$

$$\left[\, cx_{i+1} - 1 = -(cx_i - 1)^2 \,\right]$$

Calcul de $\sqrt{c}$ pour $c \in \mathbb{Z}_p^\times$

Itération de Newton

Calcul de c^{-1} pour $c \in \mathbb{Z}_p^\times$

$$f(x) = \frac{1}{x} - c \quad ; \quad f'(x) = -\frac{1}{x^2}$$

$$x_0 = c^{-1} \bmod p \quad ; \quad x_{i+1} = 2x_i - cx_i^2$$

$$\left[\, cx_{i+1} - 1 = -(cx_i - 1)^2 \,\right]$$

Calcul de $\sqrt{c}$ pour $c \in \mathbb{Z}_p^\times$

$$f(x) = x^2 - c$$

Itération de Newton

Calcul de c^{-1} pour $c \in \mathbb{Z}_p^\times$

$$f(x) = \frac{1}{x} - c \quad ; \quad f'(x) = -\frac{1}{x^2}$$

$$x_0 = c^{-1} \bmod p \quad ; \quad x_{i+1} = 2x_i - cx_i^2$$

$$\left[\, cx_{i+1} - 1 = -(cx_i - 1)^2 \,\right]$$

Calcul de $\sqrt{c}$ pour $c \in \mathbb{Z}_p^\times$

$$f(x) = x^2 - c \quad ; \quad f'(x) = 2x$$

Itération de Newton

Calcul de c^{-1} pour $c \in \mathbb{Z}_p^\times$

$$f(x) = \frac{1}{x} - c \quad ; \quad f'(x) = -\frac{1}{x^2}$$

$$x_0 = c^{-1} \bmod p \quad ; \quad x_{i+1} = 2x_i - cx_i^2$$

$$\left[\, cx_{i+1} - 1 = -(cx_i - 1)^2 \,\right]$$

Calcul de $\sqrt{c}$ pour $c \in \mathbb{Z}_p^\times$

$$f(x) = x^2 - c \quad ; \quad f'(x) = 2x$$

$$x_0 = \sqrt{c} \bmod p \quad \text{si } p > 2$$

Itération de Newton

Calcul de c^{-1} pour $c \in \mathbb{Z}_p^\times$

$$f(x) = \frac{1}{x} - c \quad ; \quad f'(x) = -\frac{1}{x^2}$$

$$x_0 = c^{-1} \bmod p \quad ; \quad x_{i+1} = 2x_i - cx_i^2$$

$$\left[\, cx_{i+1} - 1 = -(cx_i - 1)^2 \,\right]$$

Calcul de $\sqrt{c}$ pour $c \in \mathbb{Z}_p^\times$

$$f(x) = x^2 - c \quad ; \quad f'(x) = 2x$$

$$\begin{aligned} x_0 &= \sqrt{c} \bmod p \quad \text{si } p > 2 \\ &= \sqrt{c} \bmod 8 \quad \text{si } p = 2 \end{aligned}$$

Itération de Newton

Calcul de c^{-1} pour $c \in \mathbb{Z}_p^\times$

$$f(x) = \frac{1}{x} - c \quad ; \quad f'(x) = -\frac{1}{x^2}$$

$$x_0 = c^{-1} \bmod p \quad ; \quad x_{i+1} = 2x_i - cx_i^2$$

$$\left[\, cx_{i+1} - 1 = -(cx_i - 1)^2 \,\right]$$

Calcul de $\sqrt{c}$ pour $c \in \mathbb{Z}_p^\times$

$$f(x) = x^2 - c \quad ; \quad f'(x) = 2x$$

$$\begin{aligned} x_0 &= \sqrt{c} \bmod p \quad \text{si } p > 2 \\ &= \sqrt{c} \bmod 8 \quad \text{si } p = 2 \end{aligned}$$

$$x_{i+1} = \frac{1}{2} \cdot \left(x_i + \frac{c}{x_i} \right)$$

Place des nombres p-adiques en calcul formel

Place des nombres p-adiques en calcul formel

Outil $\ll$ numérique $\gg$ pour les problèmes arithmétiques

Division par p en caractéristique p

Les nombres p-adiques sont déjà là

Place des nombres p-adiques en calcul formel

Outil $\ll$ numérique $\gg$ pour les problèmes arithmétiques

- Factorisation des polynômes sur $\mathbb{Q}$

Division par p en caractéristique p

Les nombres p-adiques sont déjà là

Place des nombres p-adiques en calcul formel

Outil $\ll$ numérique $\gg$ pour les problèmes arithmétiques

- Factorisation des polynômes sur $\mathbb{Q}$
- Calcul de la forme normale de Hermite/Smith

Division par p en caractéristique p

Les nombres p-adiques sont déjà là

Place des nombres p-adiques en calcul formel

Outil $\ll$ numérique $\gg$ pour les problèmes arithmétiques

- Factorisation des polynômes sur $\mathbb{Q}$
- Calcul de la forme normale de Hermite/Smith
- Inversion de la matrice de Hilbert

Division par p en caractéristique p

Les nombres p-adiques sont déjà là

Place des nombres p-adiques en calcul formel

Outil $\ll$ numérique $\gg$ pour les problèmes arithmétiques

- Factorisation des polynômes sur $\mathbb{Q}$
- Calcul de la forme normale de Hermite/Smith
- Inversion de la matrice de Hilbert

Division par p en caractéristique p

- Résolution d'équations différentielles

Les nombres p-adiques sont déjà là

Place des nombres p-adiques en calcul formel

Outil $\ll$ numérique $\gg$ pour les problèmes arithmétiques

- Factorisation des polynômes sur $\mathbb{Q}$
- Calcul de la forme normale de Hermite/Smith
- Inversion de la matrice de Hilbert

Division par p en caractéristique p

- Résolution d'équations différentielles
- Calcul de produits composés

Les nombres p-adiques sont déjà là

Place des nombres p-adiques en calcul formel

Outil $\ll$ numérique $\gg$ pour les problèmes arithmétiques

- Factorisation des polynômes sur $\mathbb{Q}$
- Calcul de la forme normale de Hermite/Smith
- Inversion de la matrice de Hilbert

Division par p en caractéristique p

- Résolution d'équations différentielles
- Calcul de produits composés
- Calcul d'isogénies

Les nombres p-adiques sont déjà là

Place des nombres p-adiques en calcul formel

Outil « numérique » pour les problèmes arithmétiques

- Factorisation des polynômes sur $\mathbb{Q}$
- Calcul de la forme normale de Hermite/Smith
- Inversion de la matrice de Hilbert

Division par p en caractéristique p

- Résolution d'équations différentielles
- Calcul de produits composés
- Calcul d'isogénies

Les nombres p-adiques sont déjà là

- Équations différentielles p-adiques

Place des nombres p-adiques en calcul formel

Outil « numérique » pour les problèmes arithmétiques

- Factorisation des polynômes sur $\mathbb{Q}$
- Calcul de la forme normale de Hermite/Smith
- Inversion de la matrice de Hilbert

Division par p en caractéristique p

- Résolution d'équations différentielles
- Calcul de produits composés
- Calcul d'isogénies

Les nombres p-adiques sont déjà là

- Équations différentielles p-adiques
- Géométrie et cohomologies p-adiques

Place des nombres p-adiques en calcul formel

Outil « numérique » pour les problèmes arithmétiques

- Factorisation des polynômes sur $\mathbb{Q}$
- Calcul de la forme normale de Hermite/Smith
- Inversion de la matrice de Hilbert

Division par p en caractéristique p

- Résolution d'équations différentielles
- Calcul de produits composés
- Calcul d'isogénies

Les nombres p-adiques sont déjà là

- Équations différentielles p-adiques
- Géométrie et cohomologies p-adiques
- Correspondance de Langlands p-adique

Exemple : la matrice de Hilbert

Exemple : la matrice de Hilbert

La matrice de Hilbert

$$\begin{pmatrix} 1 & 1/2 & 1/3 & 1/4 \\ 1/2 & 1/3 & 1/4 & 1/5 \\ 1/3 & 1/4 & 1/5 & 1/6 \\ 1/4 & 1/5 & 1/6 & 1/7 \end{pmatrix}$$

Exemple : la matrice de Hilbert

La matrice de Hilbert

$$\begin{pmatrix} 1 & 1/2 & 1/3 & 1/4 \\ 1/2 & 1/3 & 1/4 & 1/5 \\ 1/3 & 1/4 & 1/5 & 1/6 \\ 1/4 & 1/5 & 1/6 & 1/7 \end{pmatrix}$$

Son inverse

Exemple : la matrice de Hilbert

La matrice de Hilbert

$$\begin{pmatrix} 1 & 1/2 & 1/3 & 1/4 \\ 1/2 & 1/3 & 1/4 & 1/5 \\ 1/3 & 1/4 & 1/5 & 1/6 \\ 1/4 & 1/5 & 1/6 & 1/7 \end{pmatrix}$$

Son inverse

$$\begin{pmatrix} 16 & -120 & 240 & -140 \\ -120 & 1200 & -2700 & 1680 \\ 240 & -2700 & 6480 & -4200 \\ -140 & 1680 & -4200 & 2800 \end{pmatrix}$$

Exemple : la matrice de Hilbert

La matrice de Hilbert

$$\begin{pmatrix} 1 & 1/2 & 1/3 & 1/4 \\ 1/2 & 1/3 & 1/4 & 1/5 \\ 1/3 & 1/4 & 1/5 & 1/6 \\ 1/4 & 1/5 & 1/6 & 1/7 \end{pmatrix}$$

Son inverse

$$\begin{pmatrix} 15.9999999999998 & -119.999999999997 & 239.999999999992 & 139.999999999995 \\ -119.999999999997 & 1199.99999999996 & -2699.99999999989 & 1679.99999999993 \\ 239.999999999992 & -2699.99999999989 & 6479.99999999972 & -4199.99999999981 \\ -139.999999999995 & 1679.99999999993 & -4199.99999999981 & 2799.99999999987 \end{pmatrix}$$

Exemple : la matrice de Hilbert

La matrice de Hilbert

$$\begin{pmatrix} 1 & 1/2 & 1/3 & 1/4 \\ 1/2 & 1/3 & 1/4 & 1/5 \\ 1/3 & 1/4 & 1/5 & 1/6 \\ 1/4 & 1/5 & 1/6 & 1/7 \end{pmatrix}$$

Son inverse

$$\begin{pmatrix} 15.9999999999998 & -119.999999999997 & 239.999999999992 & 139.999999999995 \\ -119.999999999997 & 1199.99999999996 & -2699.99999999989 & 1679.99999999993 \\ 239.999999999992 & -2699.99999999989 & 6479.99999999972 & -4199.99999999981 \\ -139.999999999995 & 1679.99999999993 & -4199.99999999981 & 2799.99999999987 \end{pmatrix}$$

taille de la matrice	5	6	7	8	9	10	11	12	13
nombre de chiffres corrects	40	34	28	25	19	14	9	4	0

Exemple : la matrice de Hilbert

La matrice de Hilbert

$$\begin{pmatrix} 1 & 1/2 & 1/3 & 1/4 \\ 1/2 & 1/3 & 1/4 & 1/5 \\ 1/3 & 1/4 & 1/5 & 1/6 \\ 1/4 & 1/5 & 1/6 & 1/7 \end{pmatrix}$$

Son inverse

$$\begin{pmatrix} 16 & -120 & 240 & -140 \\ -120 & 1200 & -2700 & 1680 \\ 240 & -2700 & 6480 & -4200 \\ -140 & 1680 & -4200 & 2800 \end{pmatrix}$$

Exemple : la matrice de Hilbert

La matrice de Hilbert

$$\begin{pmatrix} 1 & 1/2 & 1/3 & 1/4 \\ 1/2 & 1/3 & 1/4 & 1/5 \\ 1/3 & 1/4 & 1/5 & 1/6 \\ 1/4 & 1/5 & 1/6 & 1/7 \end{pmatrix}$$

Son inverse

$$\begin{pmatrix} \ldots 000000000001000 & \ldots 111111110001000 & \ldots 000000011110000 & \ldots 111111101110100 \\ \ldots 111111110001000 & \ldots 000010010110000 & \ldots 111010101110100 & \ldots 000011010010000 \\ \ldots 000000011110000 & \ldots 111010101110100 & \ldots 001100101010000 & \ldots 110111110011000 \\ \ldots 111111101110100 & \ldots 000011010010000 & \ldots 110111110011000 & \ldots 000101011110000 \end{pmatrix}$$

Exemple : la matrice de Hilbert

La matrice de Hilbert

$$\begin{pmatrix} 1 & 1/2 & 1/3 & 1/4 \\ 1/2 & 1/3 & 1/4 & 1/5 \\ 1/3 & 1/4 & 1/5 & 1/6 \\ 1/4 & 1/5 & 1/6 & 1/7 \end{pmatrix}$$

Son inverse

$$\begin{pmatrix} \ldots 000000000001000 & \ldots 111111110001000 & \ldots 000000011110000 & \ldots 111111101110100 \\ \ldots 111111110001000 & \ldots 000010010110000 & \ldots 111010101110100 & \ldots 000011010010000 \\ \ldots 000000011110000 & \ldots 111010101110100 & \ldots 001100101010000 & \ldots 110111110011000 \\ \ldots 111111101110100 & \ldots 000011010010000 & \ldots 110111110011000 & \ldots 000101011110000 \end{pmatrix}$$

taille de la matrice	5	6	7	8	9	10	11	12	13	100
nombre de chiffres corrects	52	52	51	51	51	51	51	51	51	48

Deuxième partie

Implémentation des nombres p-adiques

L’arithmétique zélée

L’arithmétique zélée

Représentation

L'arithmétique zélée

Représentation

$$a + O(p^N)$$

L'arithmétique zélée

Représentation

$$a + O(p^N) \quad = \quad \ldots a_{N-1} a_{N-2} \ldots a_1 a_0 \, , \, a_{-1} a_{-2} \ldots$$

L'arithmétique zélée

Représentation

$$\begin{aligned} a + O(p^N) &= \ldots a_{N-1} a_{N-2} \ldots a_1 a_0 \, , \, a_{-1} a_{-2} \ldots \\ 2017 + O(2^{12}) &= \ldots 011111100001 \end{aligned}$$

L'arithmétique zélée

Représentation

$$\begin{aligned} a + O(p^N) &= \ldots a_{N-1} a_{N-2} \ldots a_1 a_0 \, , \, a_{-1} a_{-2} \ldots \\ 2017 + O(2^{12}) &= \ldots 011111100001 \end{aligned}$$

Opérations

L'arithmétique zélée

Représentation

$$\begin{aligned} a + O(p^N) &= \ldots a_{N-1} a_{N-2} \ldots a_1 a_0 \,,\, a_{-1} a_{-2} \ldots \\ 2017 + O(2^{12}) &= \ldots 011111100001 \end{aligned}$$

Opérations

$$\left(a + O(p^N)\right) + \left(a' + O(p^{N'})\right) = a + a' + O\left(p^{\min(N, N')}\right)$$

L'arithmétique zélée

Représentation

$$\begin{aligned} a + O(p^N) &= \ldots a_{N-1} a_{N-2} \ldots a_1 a_0 \,,\, a_{-1} a_{-2} \ldots \\ 2017 + O(2^{12}) &= \ldots 011111100001 \end{aligned}$$

Opérations

$$\begin{aligned} (a + O(p^N)) + (a' + O(p^{N'})) &= a + a' + O\big(p^{\min(N, N')}\big) \\ (a + O(p^N)) - (a' + O(p^{N'})) &= a - a' + O\big(p^{\min(N, N')}\big) \end{aligned}$$

L'arithmétique zélée

Représentation

$$\begin{aligned} a + O(p^N) &= \ldots a_{N-1} a_{N-2} \ldots a_1 a_0 \,,\, a_{-1} a_{-2} \ldots \\ 2017 + O(2^{12}) &= \ldots 011111100001 \end{aligned}$$

Opérations

$$\begin{aligned} (a + O(p^N)) + (a' + O(p^{N'})) &= a + a' + O\big(p^{\min(N,\, N')}\big) \\ (a + O(p^N)) - (a' + O(p^{N'})) &= a - a' + O\big(p^{\min(N,\, N')}\big) \end{aligned}$$

$$\begin{aligned} (a + O(p^N)) \times (a' + O(p^{N'})) &= aa' + O\big(p^{\min(v+N',\, N+v')}\big) \\ (a + O(p^N)) \div (a' + O(p^{N'})) &= \tfrac{a}{a'} + O\big(p^{\min(v+N'-2v',\, N-v')}\big) \end{aligned}$$

$$\big[\, v = \mathrm{val}(a),\ v' = \mathrm{val}(a') \,\big]$$

L’arithmétique paresseuse

L’arithmétique paresseuse

Représentation

L'arithmétique paresseuse

Représentation

```
def x(N):
    # return an approximation of x at precision O(p^N)
```

L'arithmétique paresseuse

Représentation

```
def x(N):
    # return an approximation of x at precision O(p^N)
```

Opérations

L'arithmétique paresseuse

Représentation

```
def x(N):
    # return an approximation of x at precision O(p^N)
```

Opérations

```
def x_plus_y(N):
    return x(N) + y(N)
```

L'arithmétique paresseuse

Représentation

```
def x(N):
    # return an approximation of x at precision O(p^N)
```

Opérations

```
def x_plus_y(N):
    return x(N) + y(N)
```

L'arithmétique paresseuse

Représentation

```
def x(N):
    # return an approximation of x at precision O(p^N)
```

Opérations

```
def add(x,y):
    def x_plus_y(N):
        return x(N) + y(N)
    return x_plus_y
```

L'arithmétique paresseuse

Représentation

```
def x(N):
    # return an approximation of x at precision O(p^N)
```

Opérations

```
def add(x,y):
    def x_plus_y(N):
        return x(N) + y(N)
    return x_plus_y

def x_moins_y(N):
    return x(N) - y(N)
```

L’arithmétique paresseuse

Opérations

L'arithmétique paresseuse

Opérations

```
def x_fois_y(x,y):
    vx = val(x)
    vy = val(y)
    return x(N-vy) * y(N-vx)
```

L'arithmétique paresseuse

Opérations

```
def x_fois_y(x,y):
    vx = val(x)
    vy = val(y)
    return x(N-vy) * y(N-vx)
```

$$(a + O(p^N)) \times (a' + O(p^{N'})) = aa' + O(p^{\min(v+N', N+v')})$$

L'arithmétique paresseuse

Opérations

```
def x_fois_y(x,y):
    vx = val(x)
    vy = val(y)
    return x(N-vy) * y(N-vx)

def val(x):
    for N in ℕ:
        v = val_p(x(N))
        if v < N: return v
    return ∞
```

L'arithmétique paresseuse

Opérations

```
def x_fois_y(x,y):
    vx = min(0, val_p(x(0)))
    vy = min(0, val_p(y(0)))
    return x(N-vy) * y(N-vx)

def val(x):
    for N in ℕ:
        v = val_p(x(N))
        if v < N: return v
    return ∞
```

L'arithmétique paresseuse

Opérations

```
def x_sur_y(x,y):
    vx = min(0, val_p(x(0)))
    vy = val(y)
    return x(N+vy) / y(N+2*vy-vx)

def val(x):
    for N in ℕ:
        v = val_p(x(N))
        if v < N: return v
    return ∞
```

L’arithmétique détendue

L’arithmétique détendue

Représentation

L'arithmétique détendue

Représentation

```
class RelaxedPAdicInteger:
    # Variable
    digits          # list of (already computed) digits

    # Virtual method
    def next(self)
        # compute the next digit and append it to the list
```

L'arithmétique détendue

Représentation

```
class RelaxedPAdicInteger:
    # Variable
    digits          # list of (already computed) digits

    # Virtual method
    def next(self)
        # compute the next digit and append it to the list

    def __getitem__(self,N):
        n = len(self.digits)
        while n < N+1:
            self.next()
            n += 1
        return self.digits[N]
```

L’arithmétique détendue

Opérations

L'arithmétique détendue

Opérations

```
class x_plus_y(RelaxedPAdicInteger):
    # Additional variable
    carry           # the current carry

    def next(self):
        n = len(self.digits)
        s = x[n] + y[n] + self.carry
        self.digits[n] = s % p
        self.carry = s // p
```

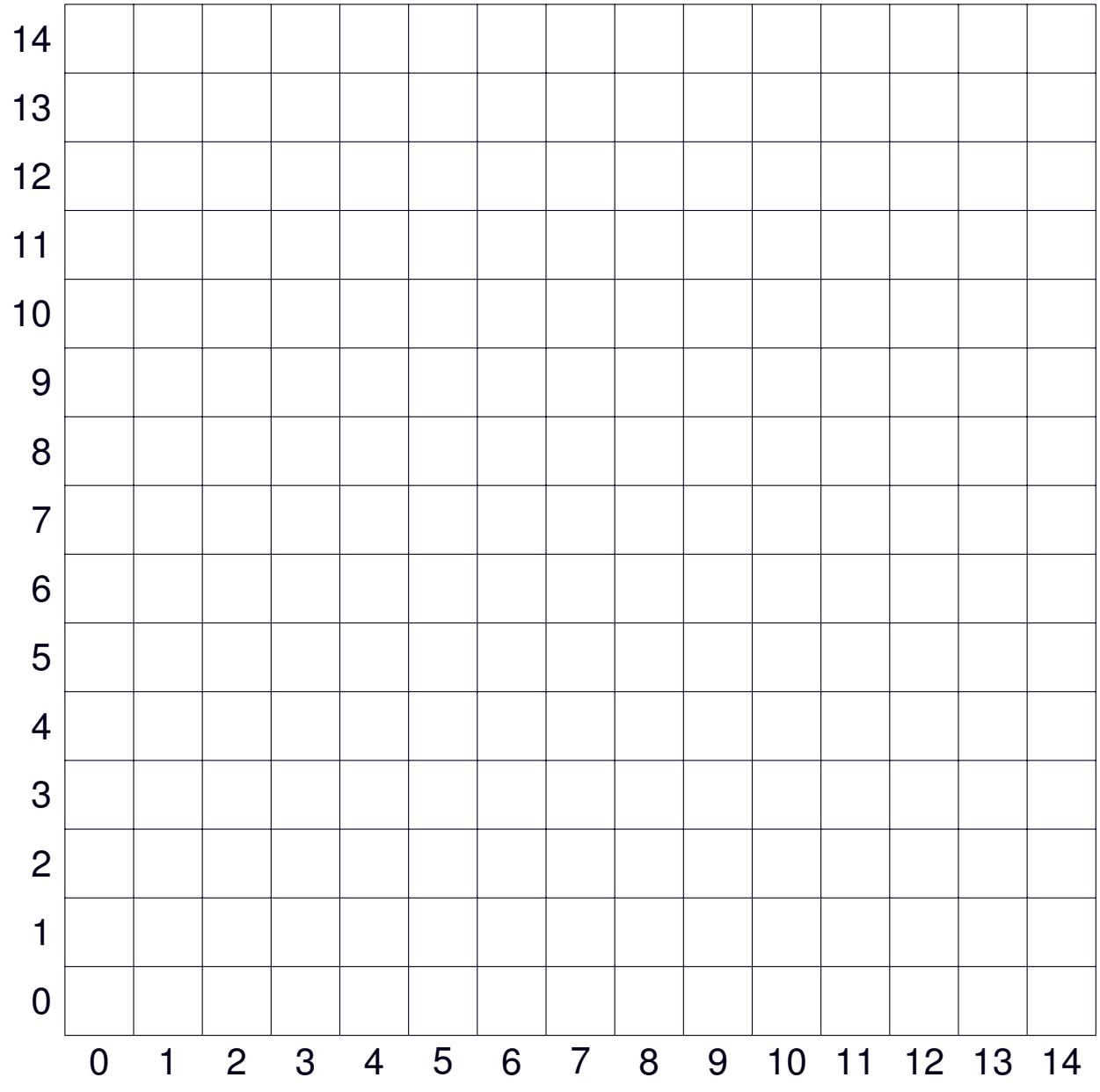
L'arithmétique détendue

Opérations

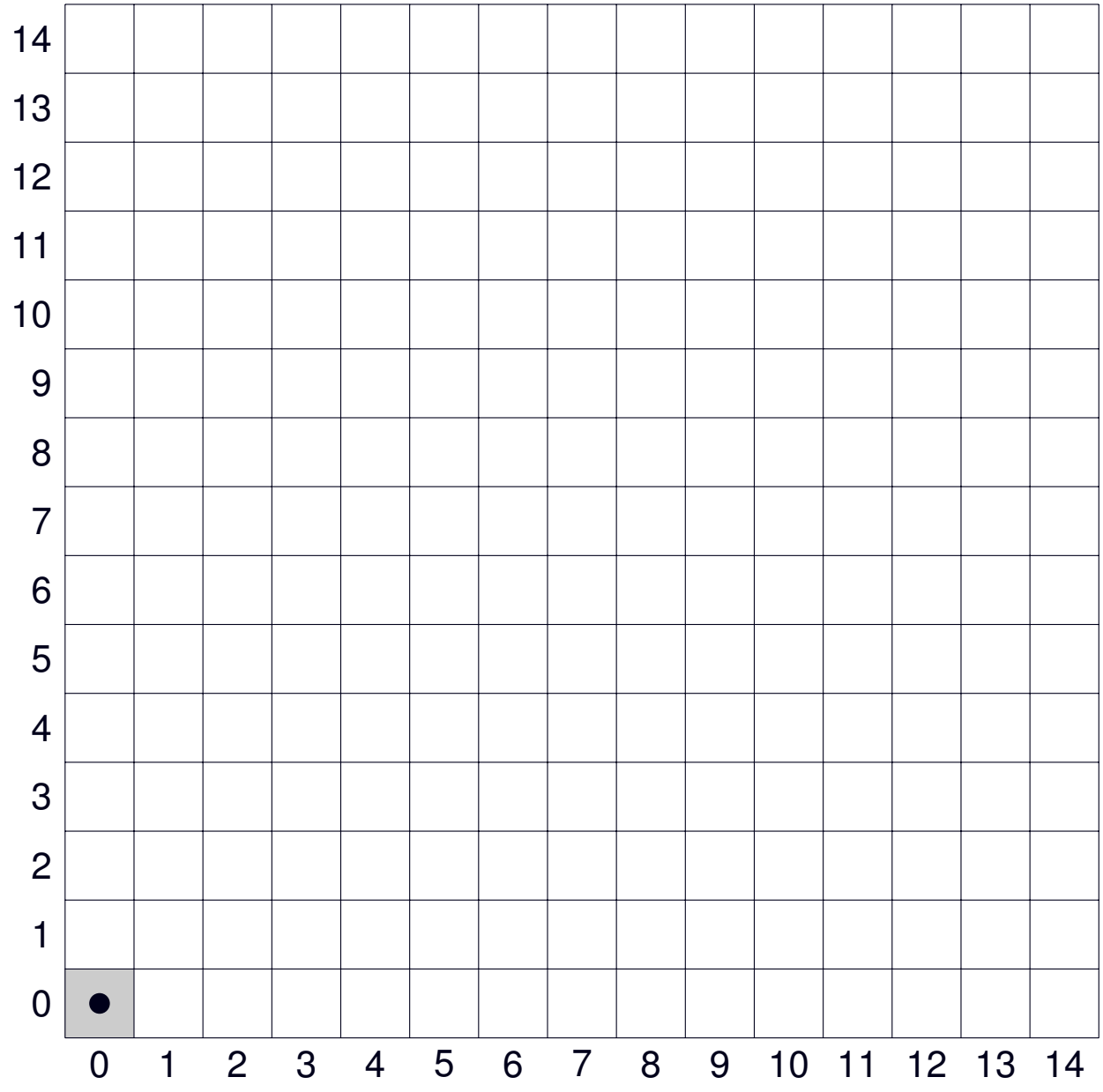
```
class x_fois_y(RelaxedPAdicInteger):
    # Additional variable
    carry           # the current carry

    def next(self):
        n = len(self.digits)
        s = self.carry
        for i in 0,1,...,n:
            s += x[i] * y[n-i]
        self.digits[n] = s % p
        self.carry = s // p
```

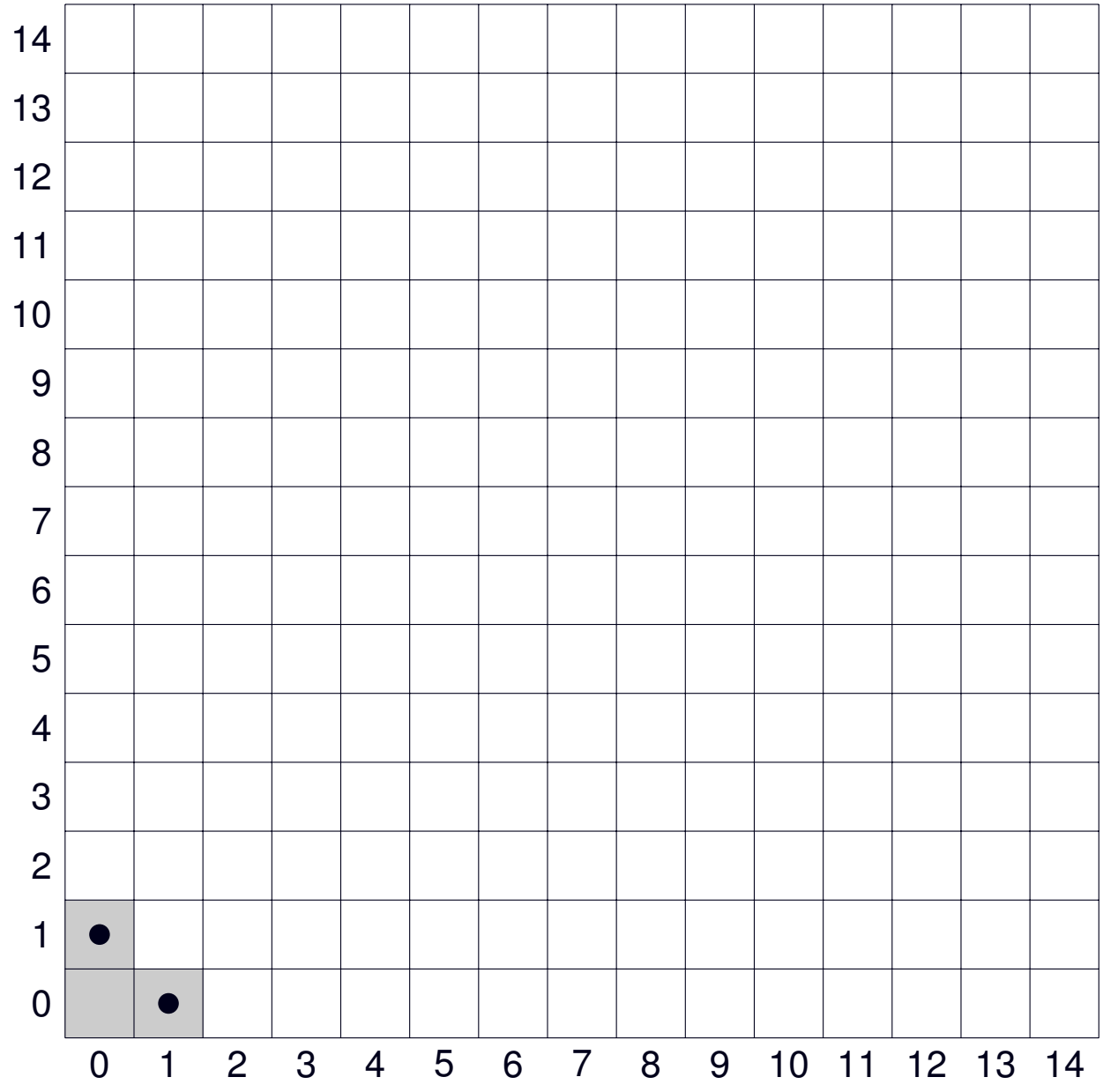
L’arithmétique détendue



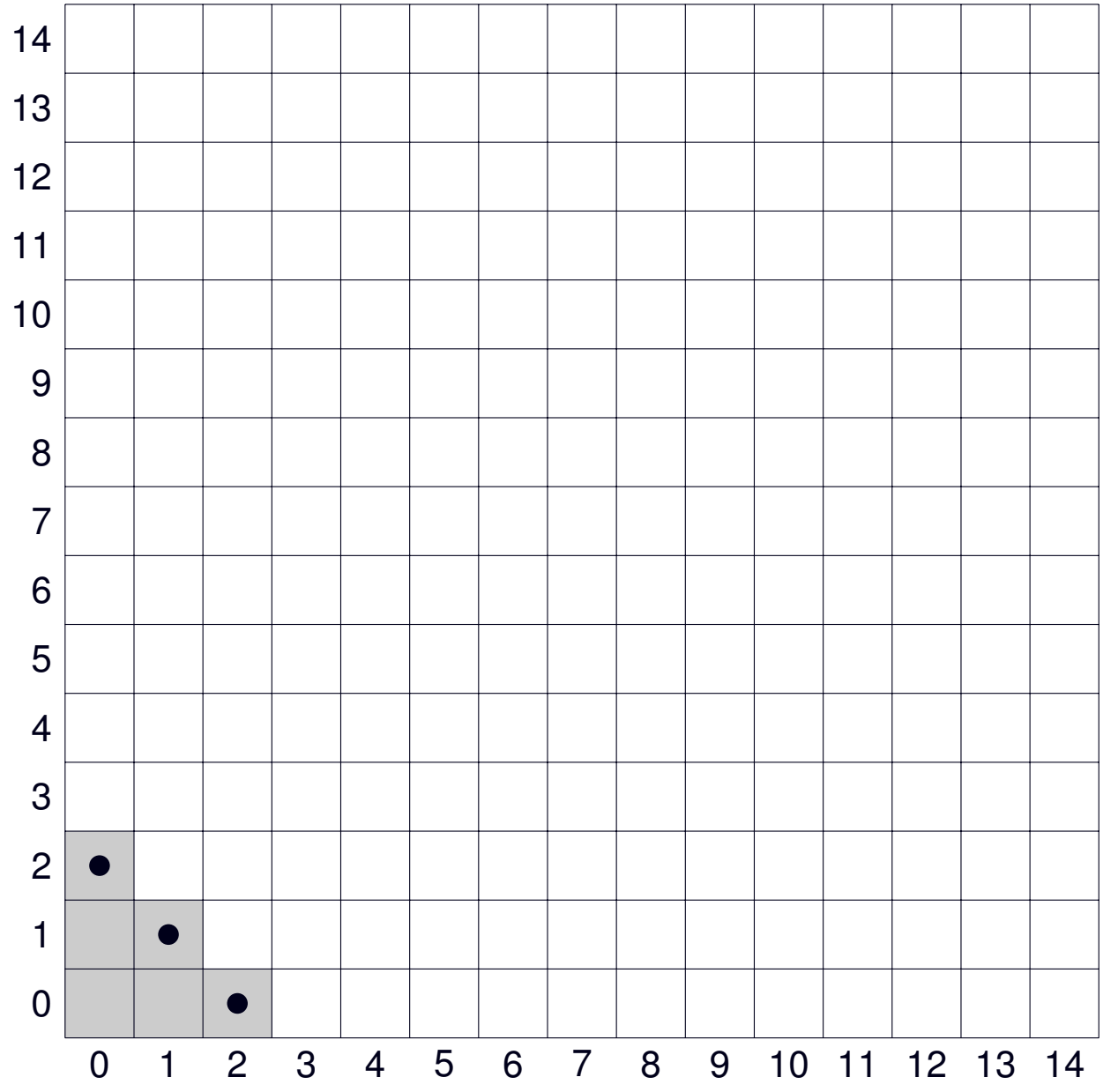
L’arithmétique détendue



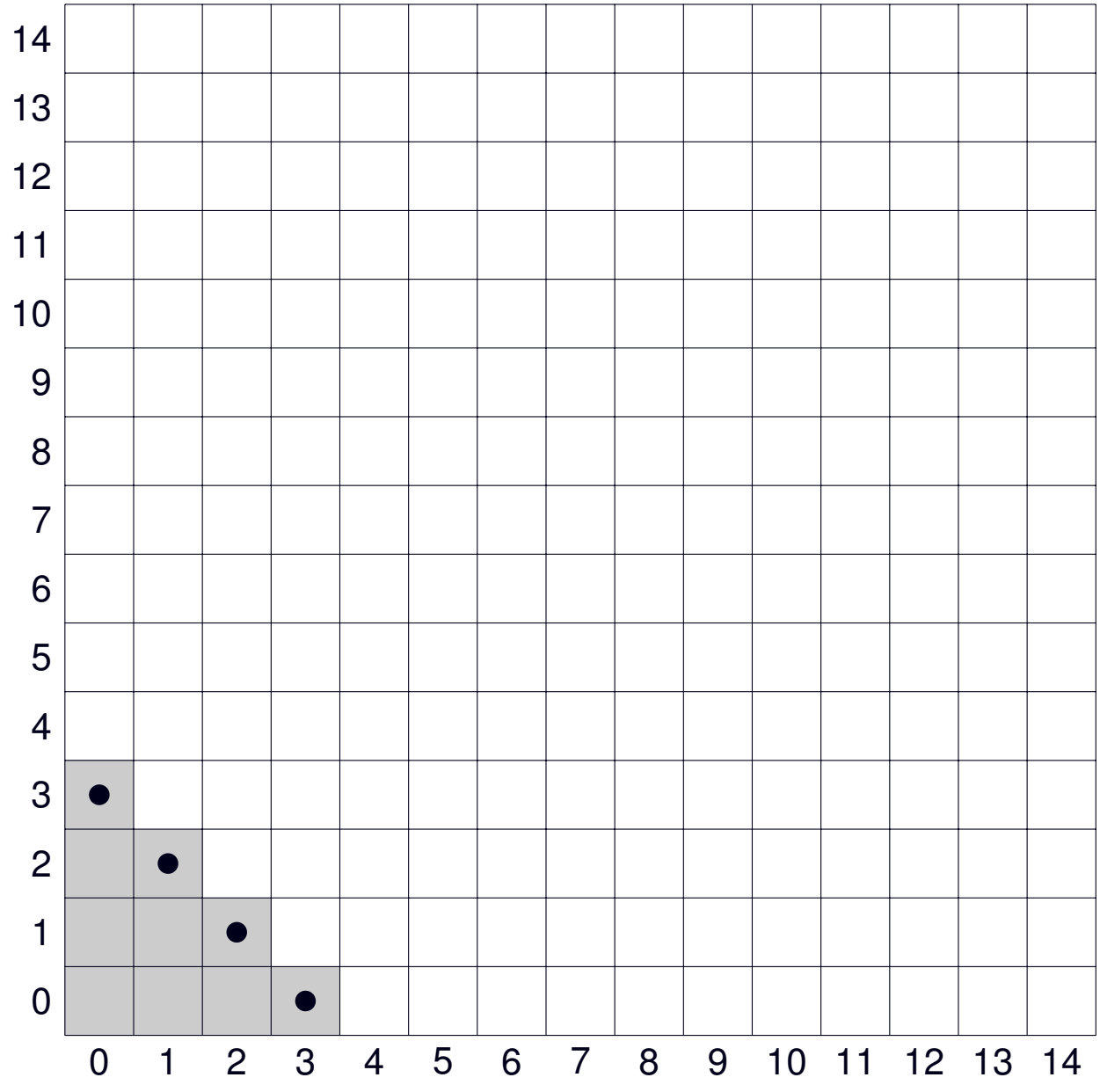
L’arithmétique détendue



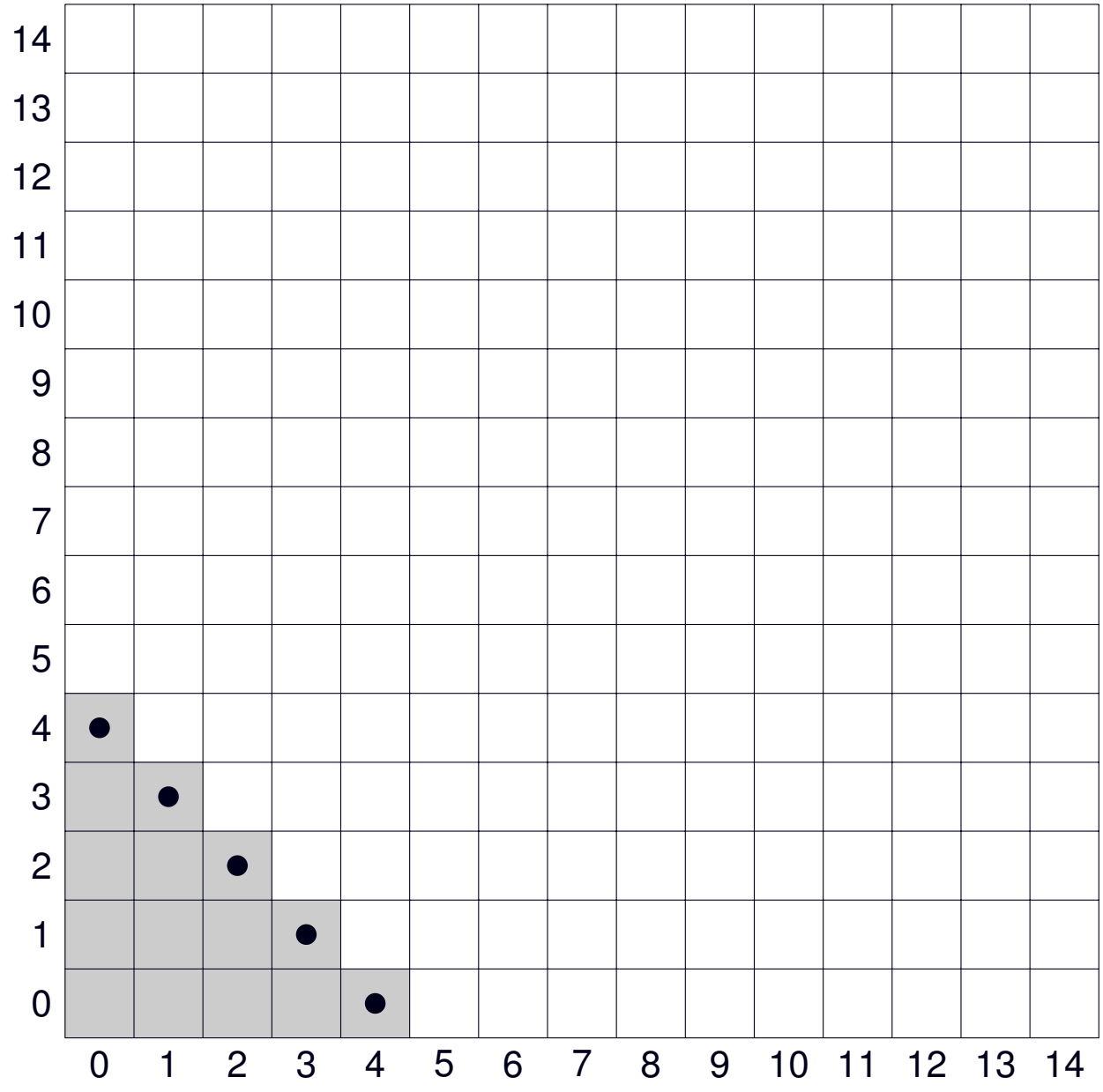
L’arithmétique détendue



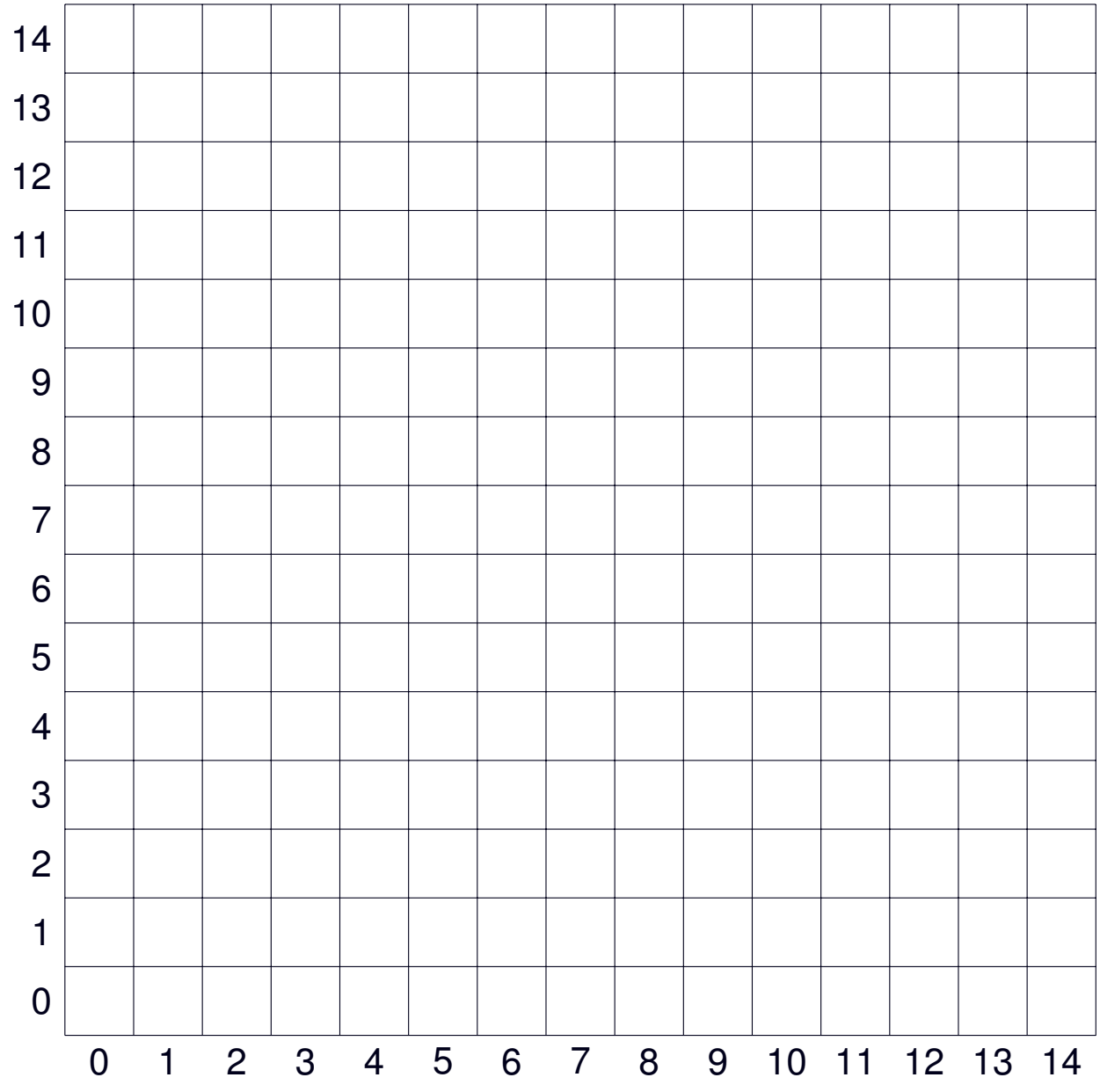
L’arithmétique détendue



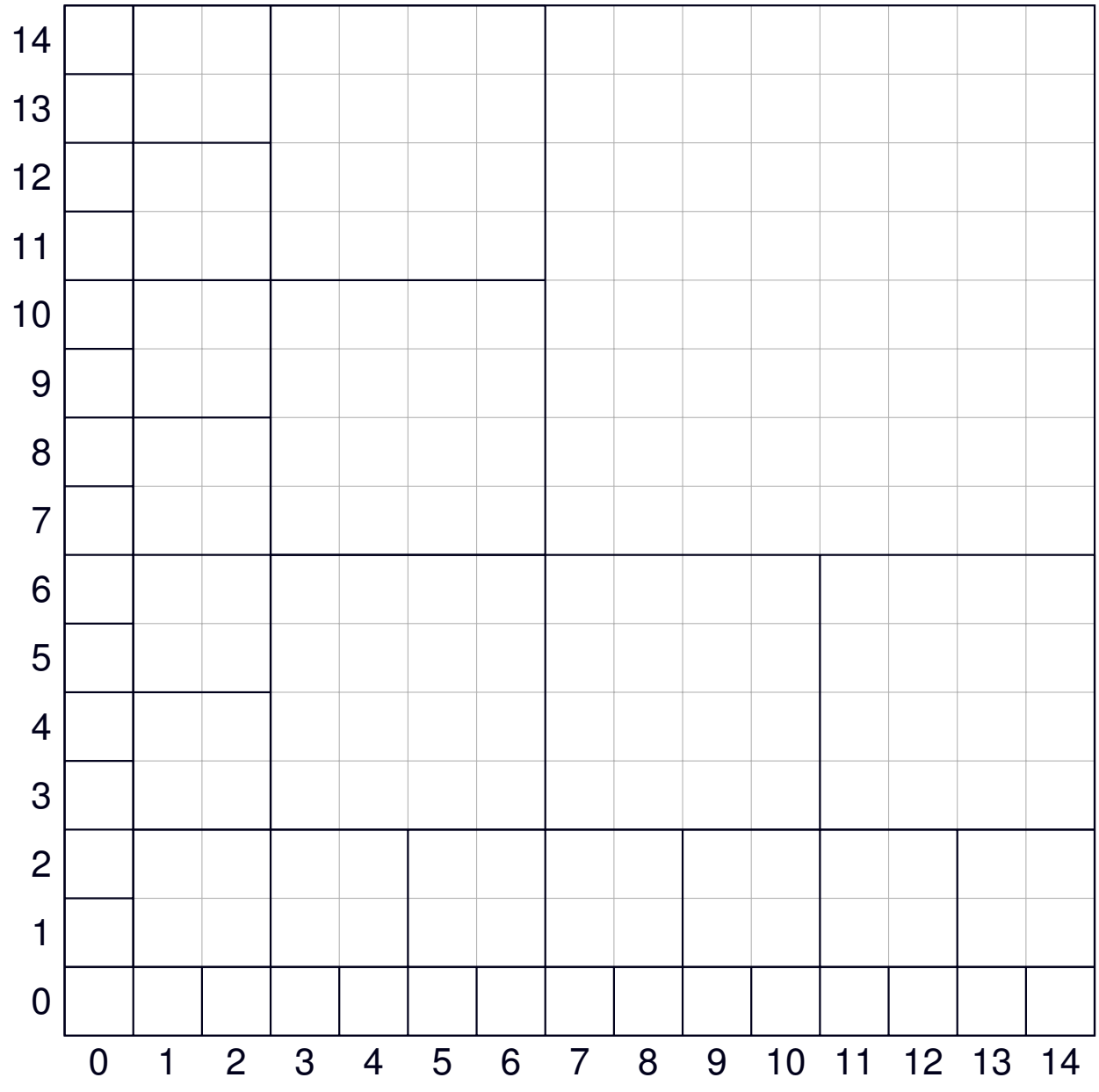
L’arithmétique détendue



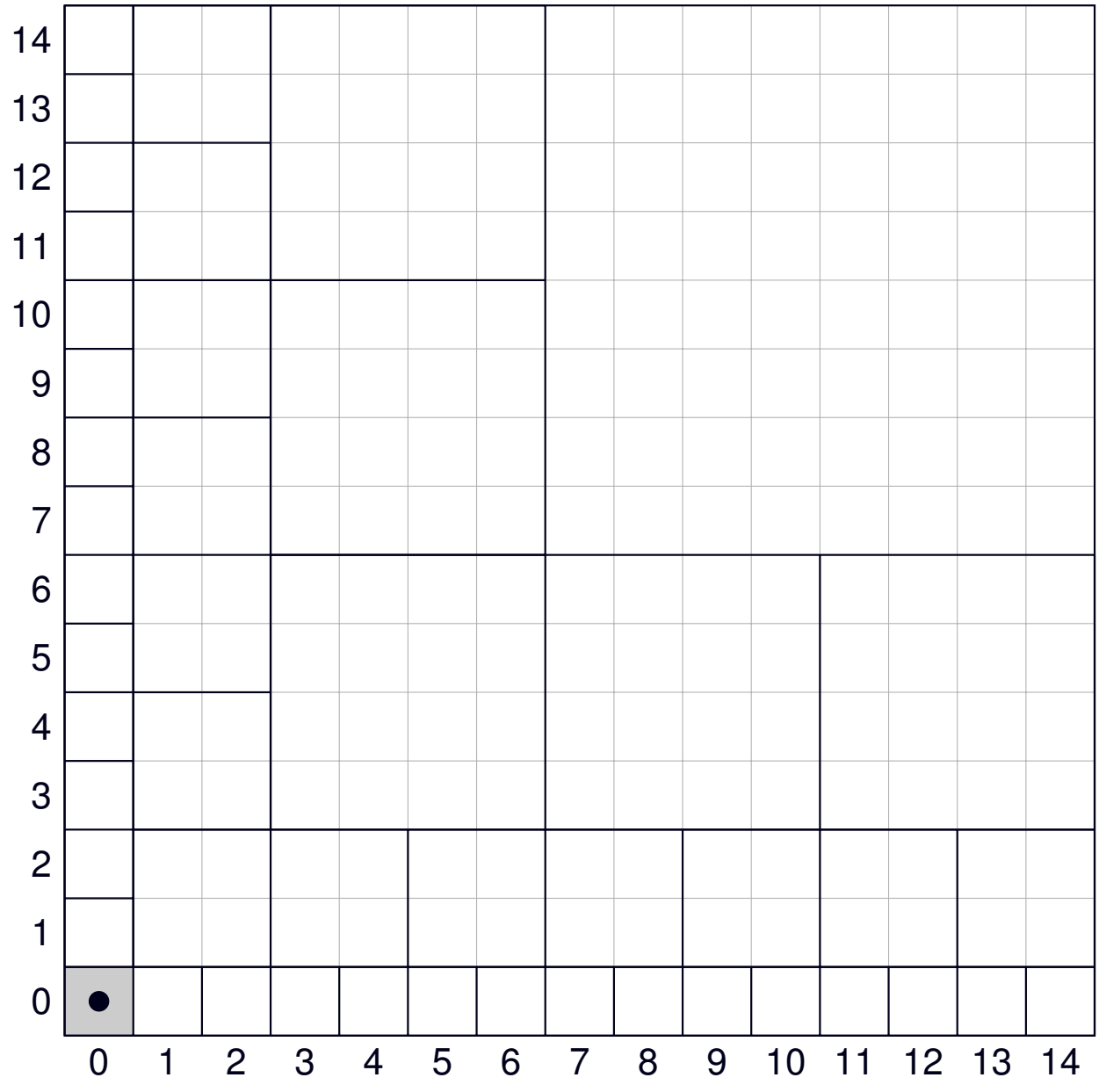
L’arithmétique détendue



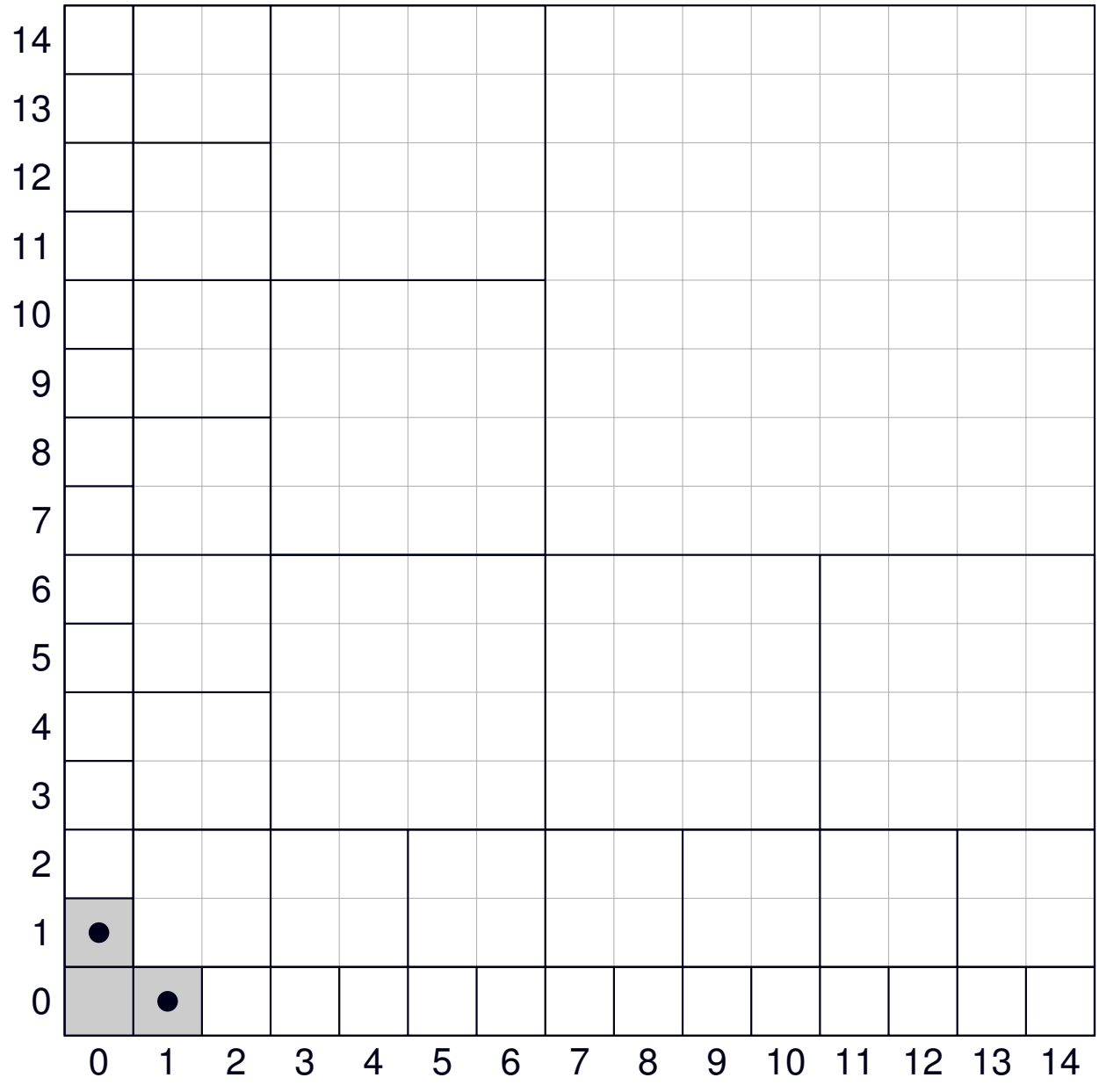
L’arithmétique détendue



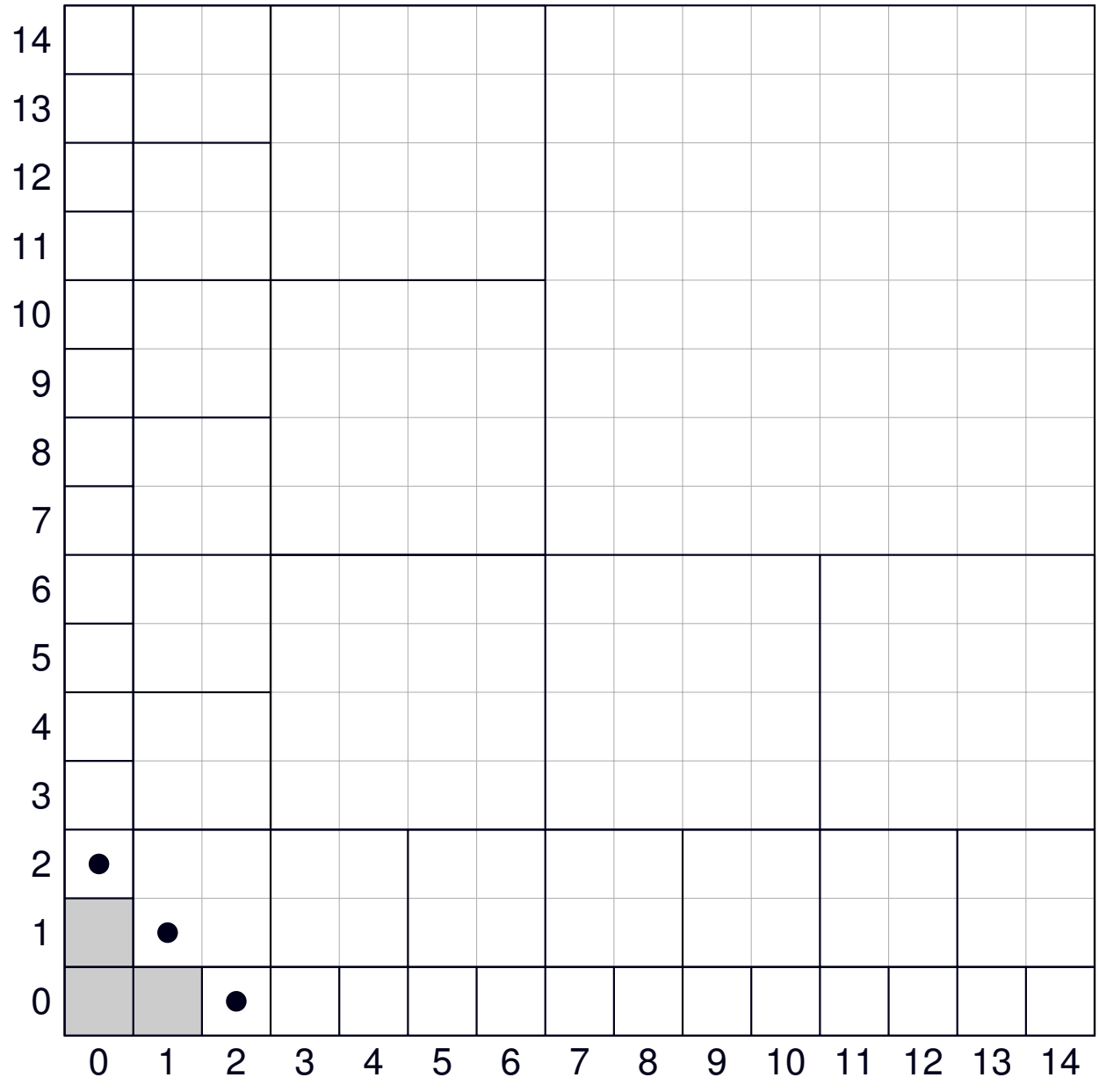
L’arithmétique détendue



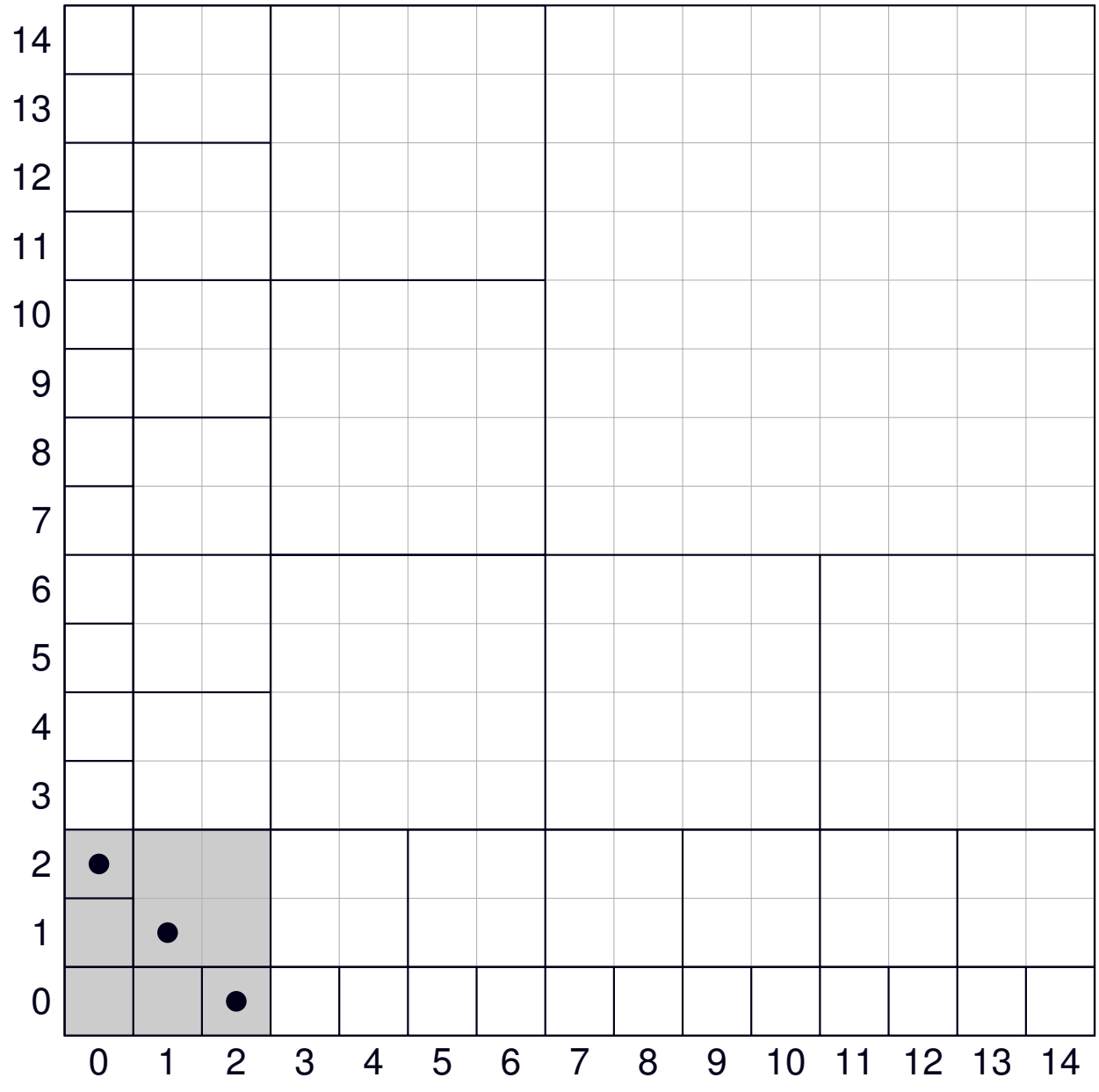
L’arithmétique détendue



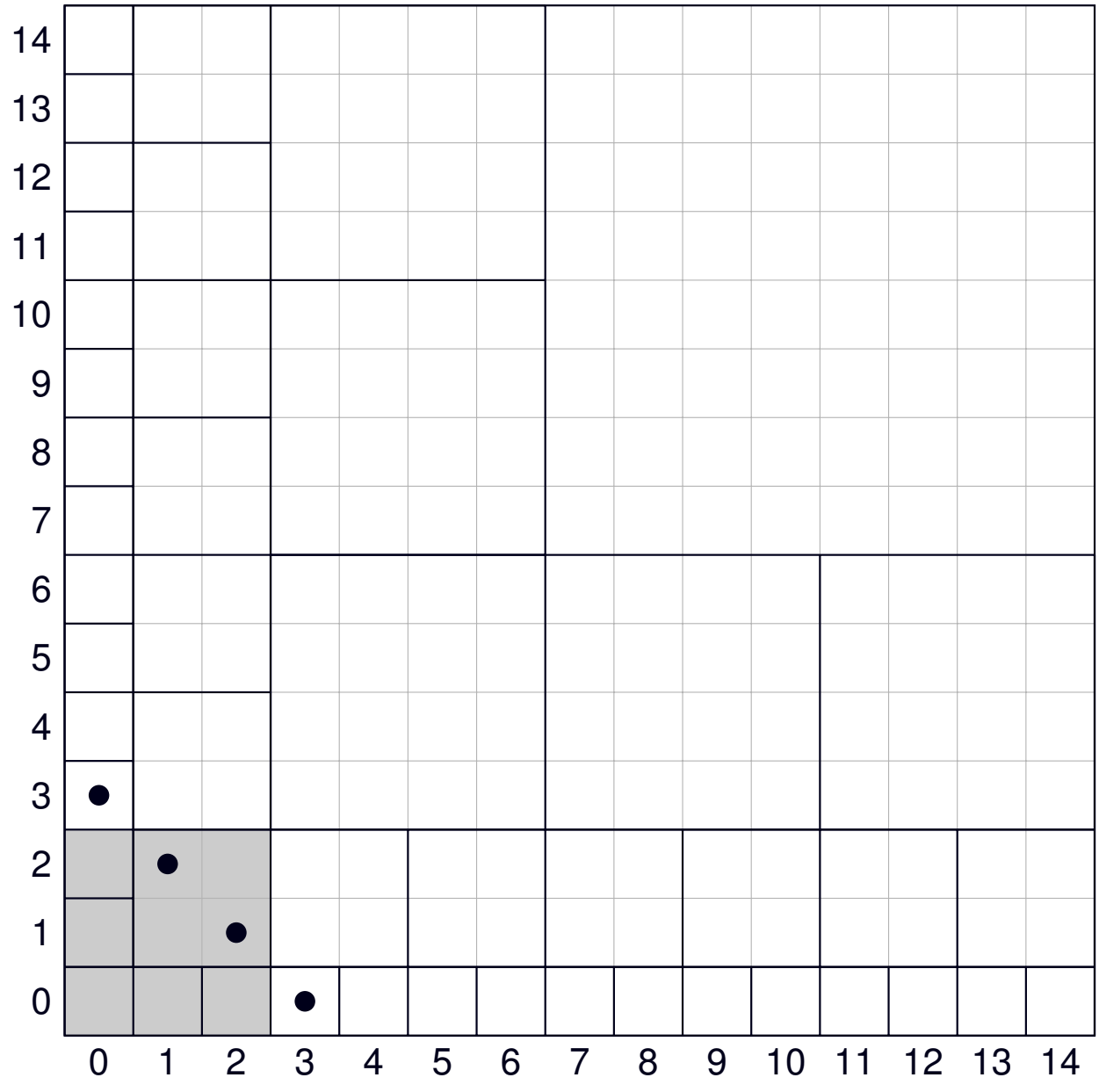
L’arithmétique détendue



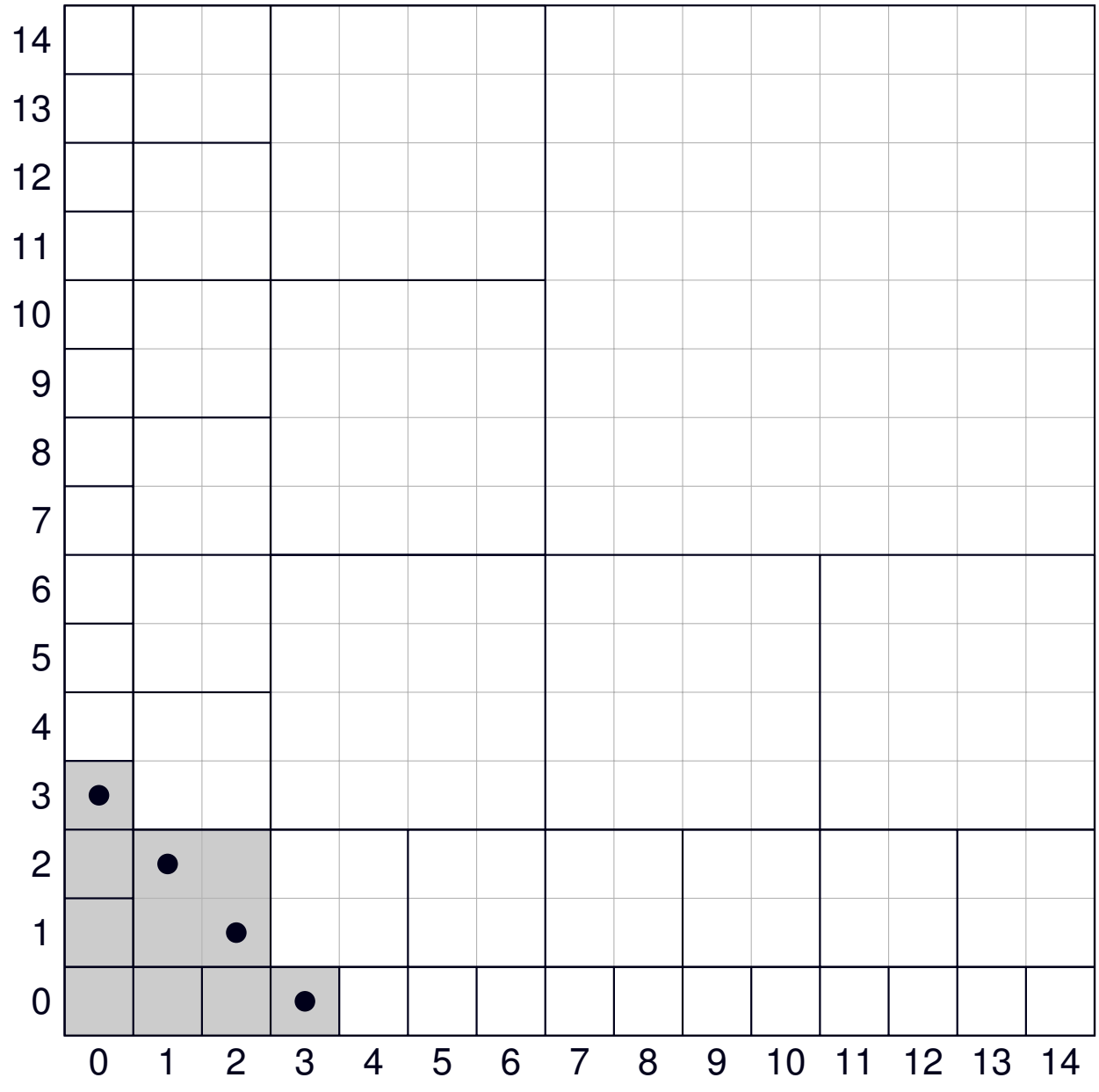
L’arithmétique détendue



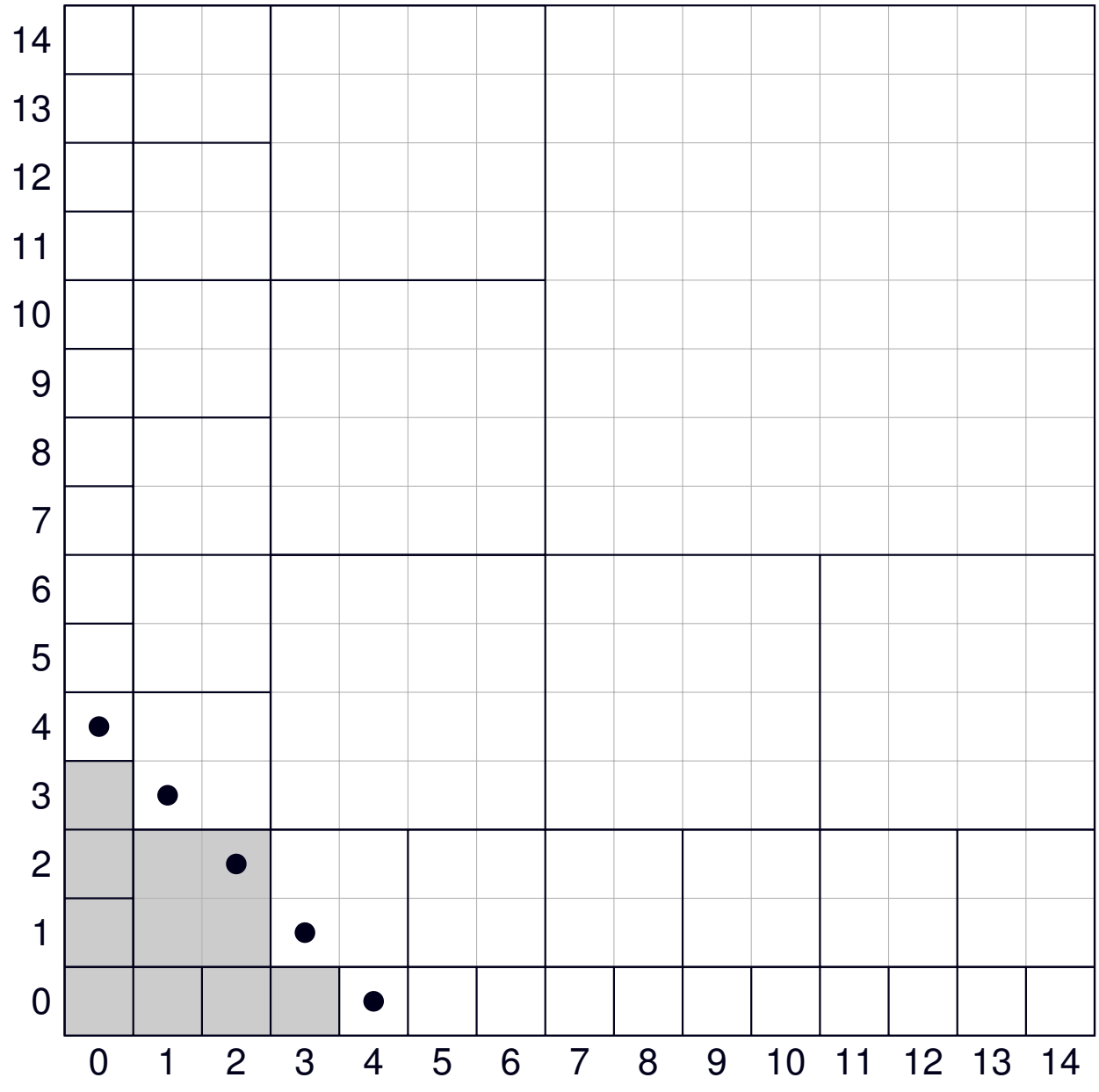
L’arithmétique détendue



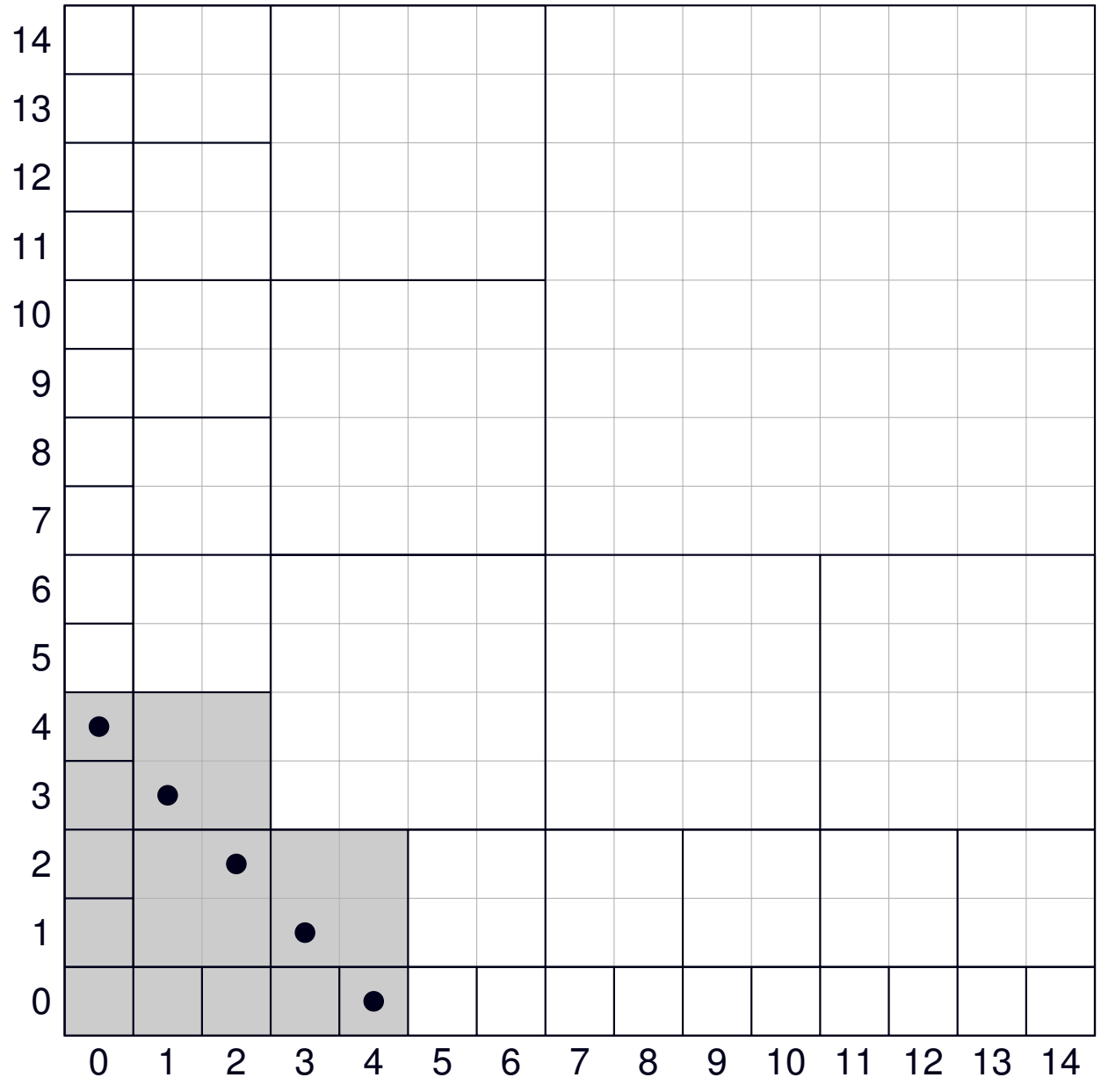
L’arithmétique détendue



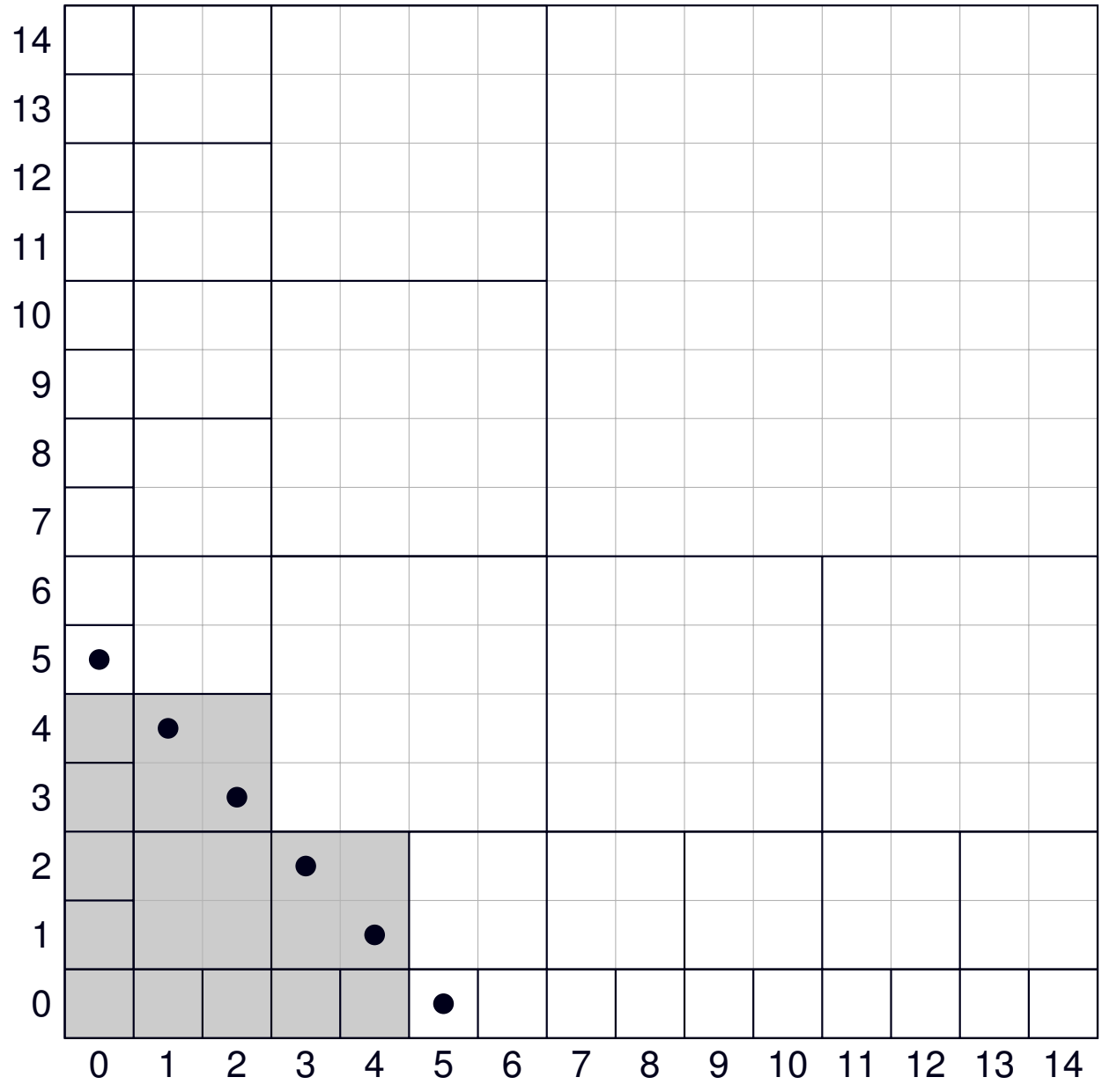
L’arithmétique détendue



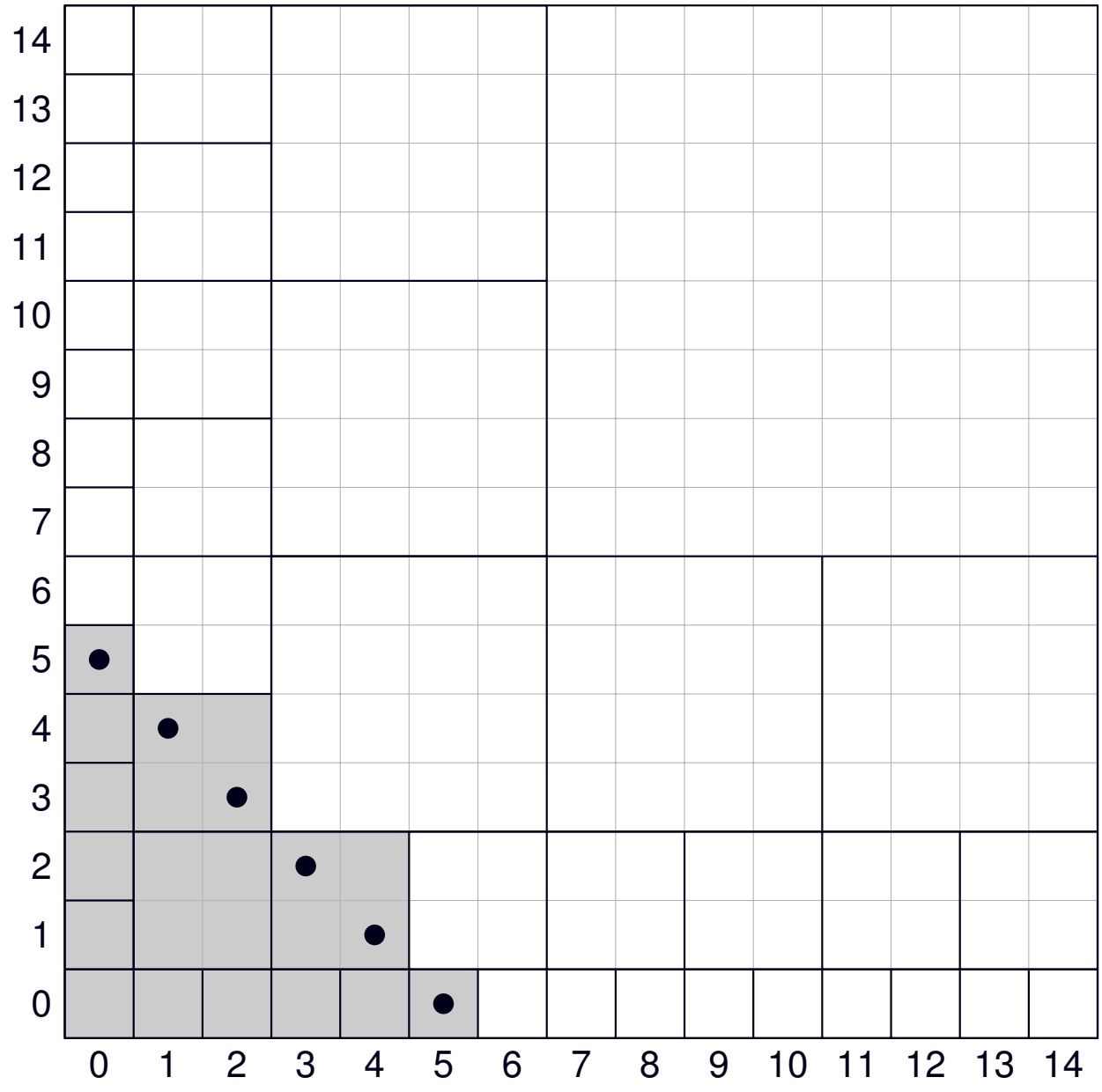
L’arithmétique détendue



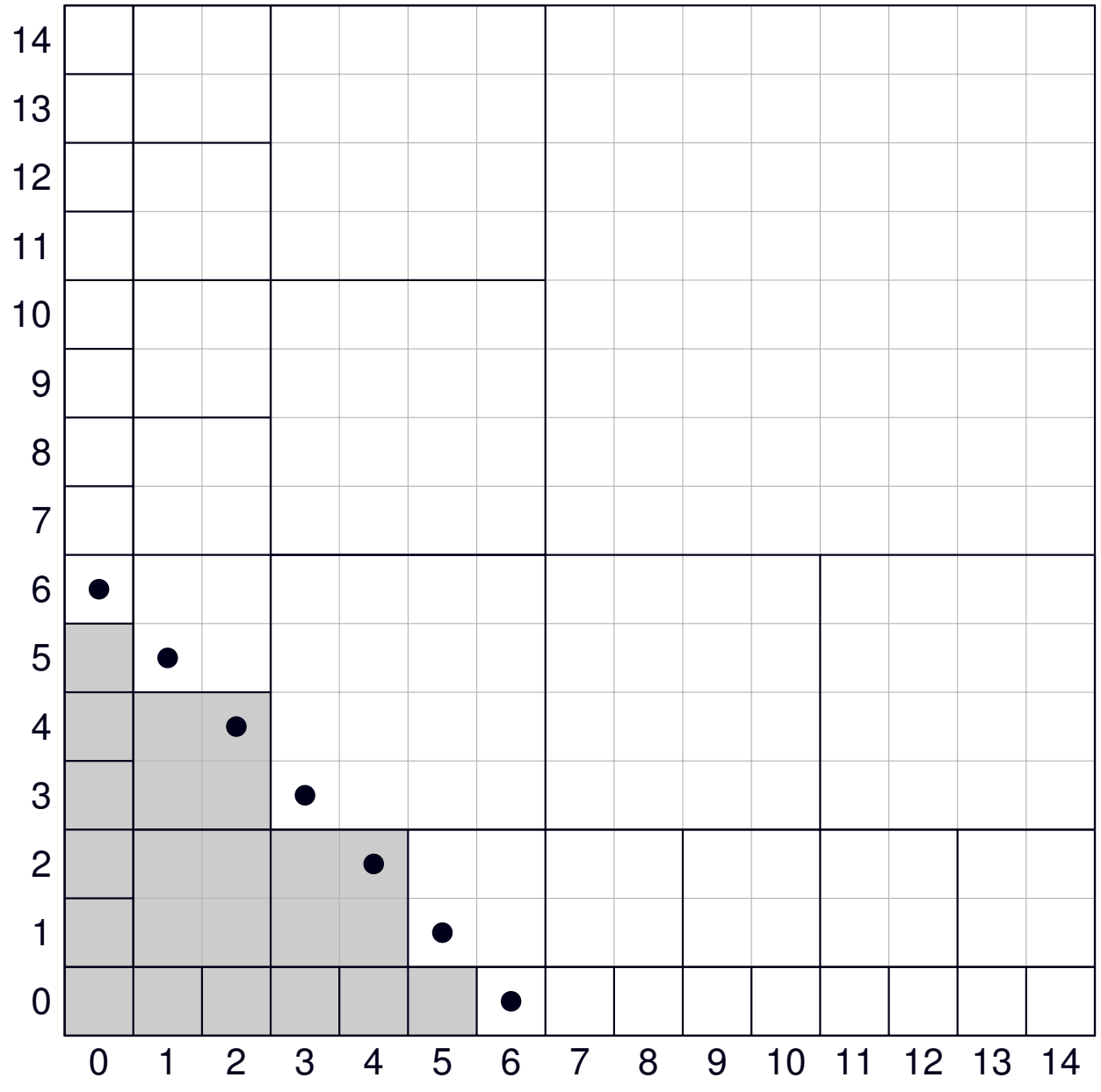
L’arithmétique détendue



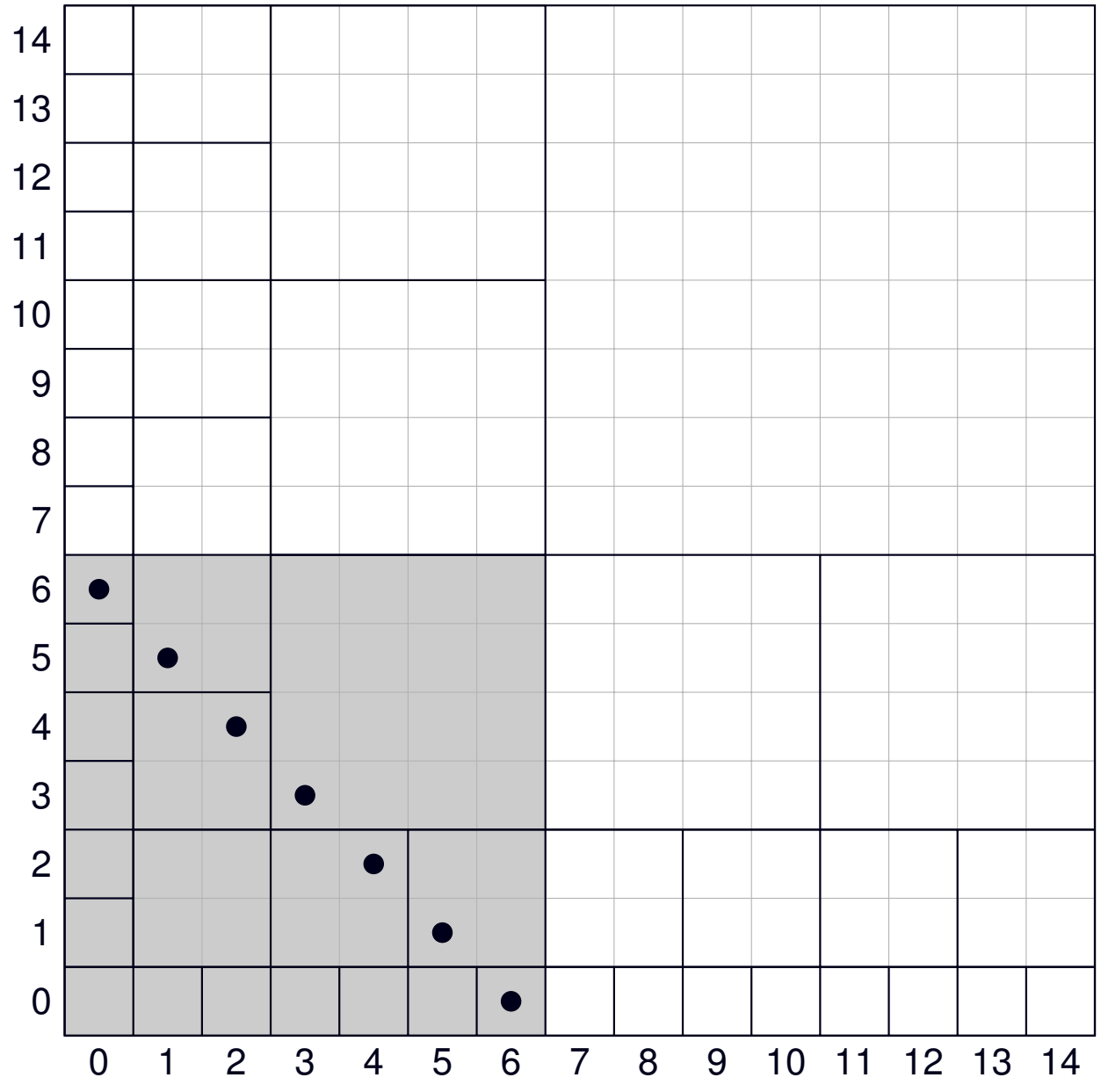
L’arithmétique détendue



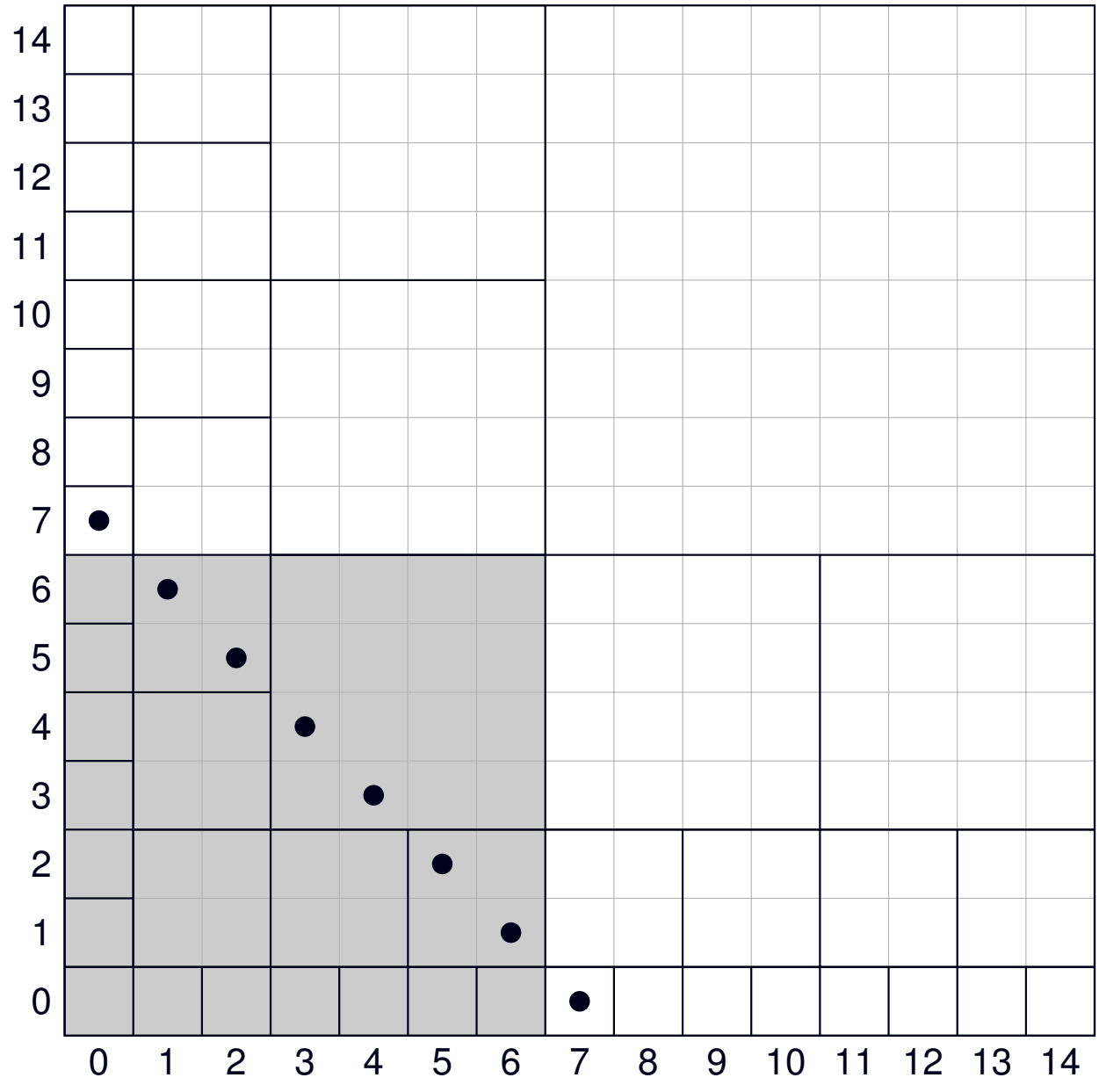
L’arithmétique détendue



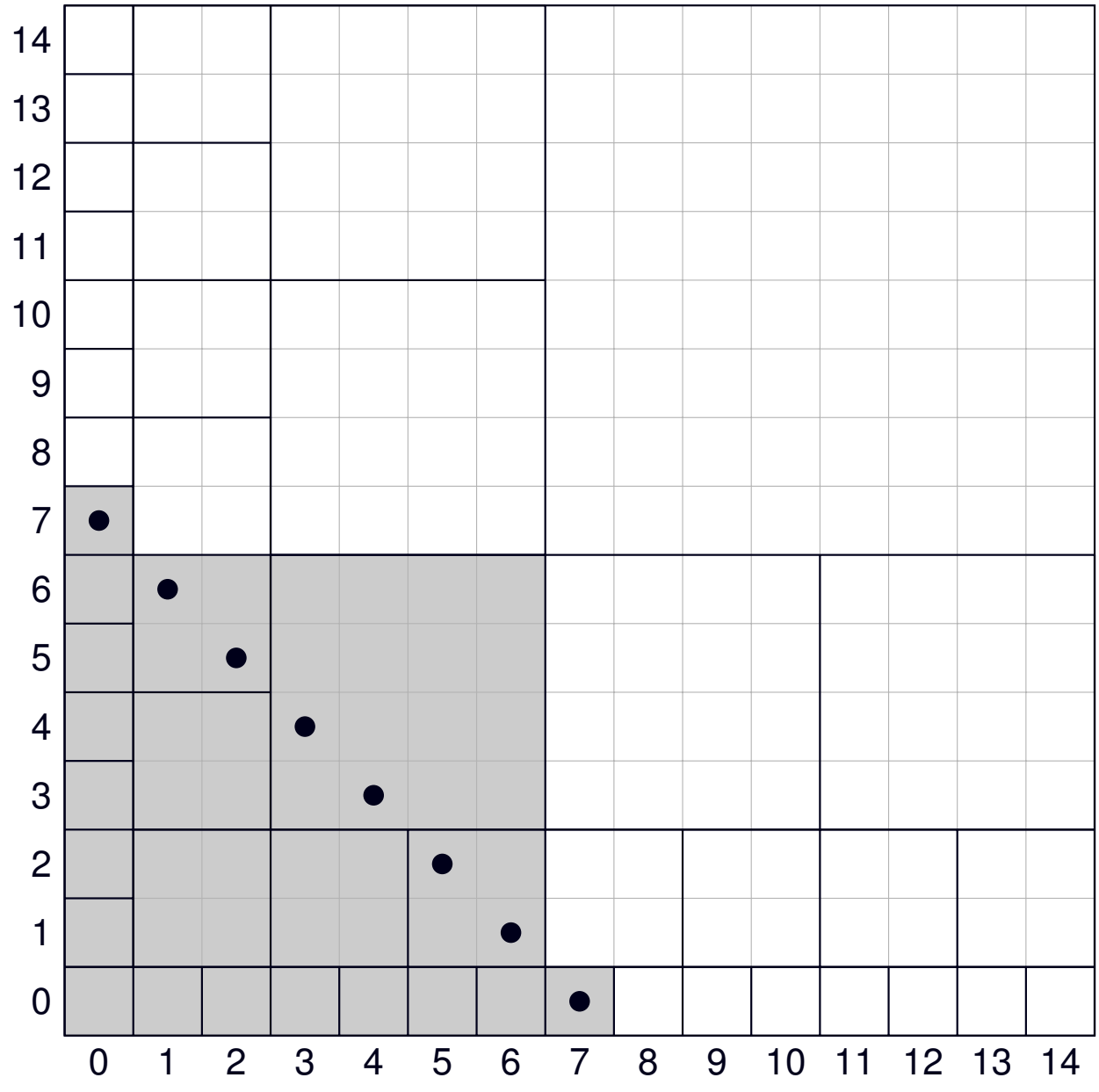
L’arithmétique détendue



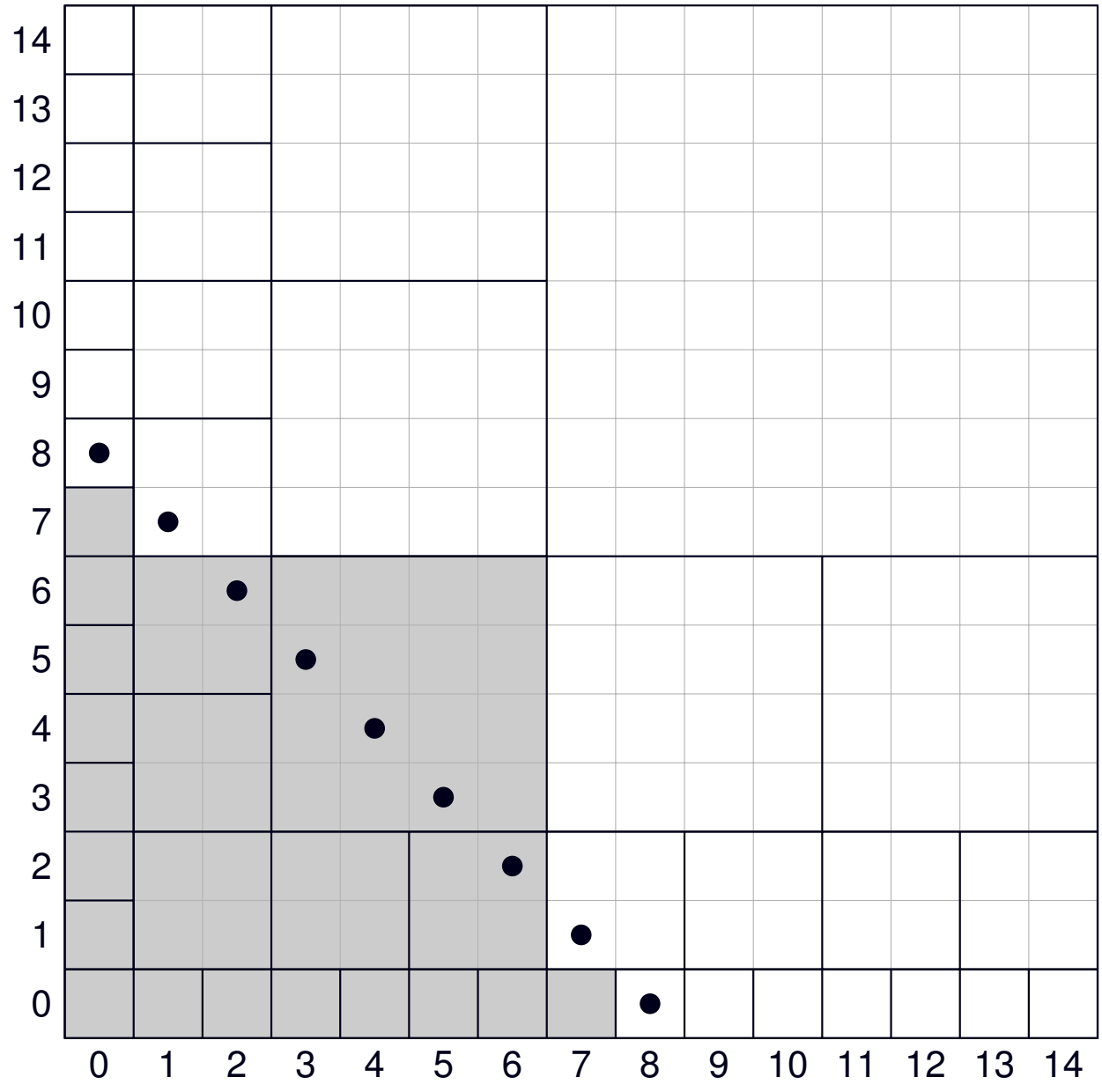
L’arithmétique détendue



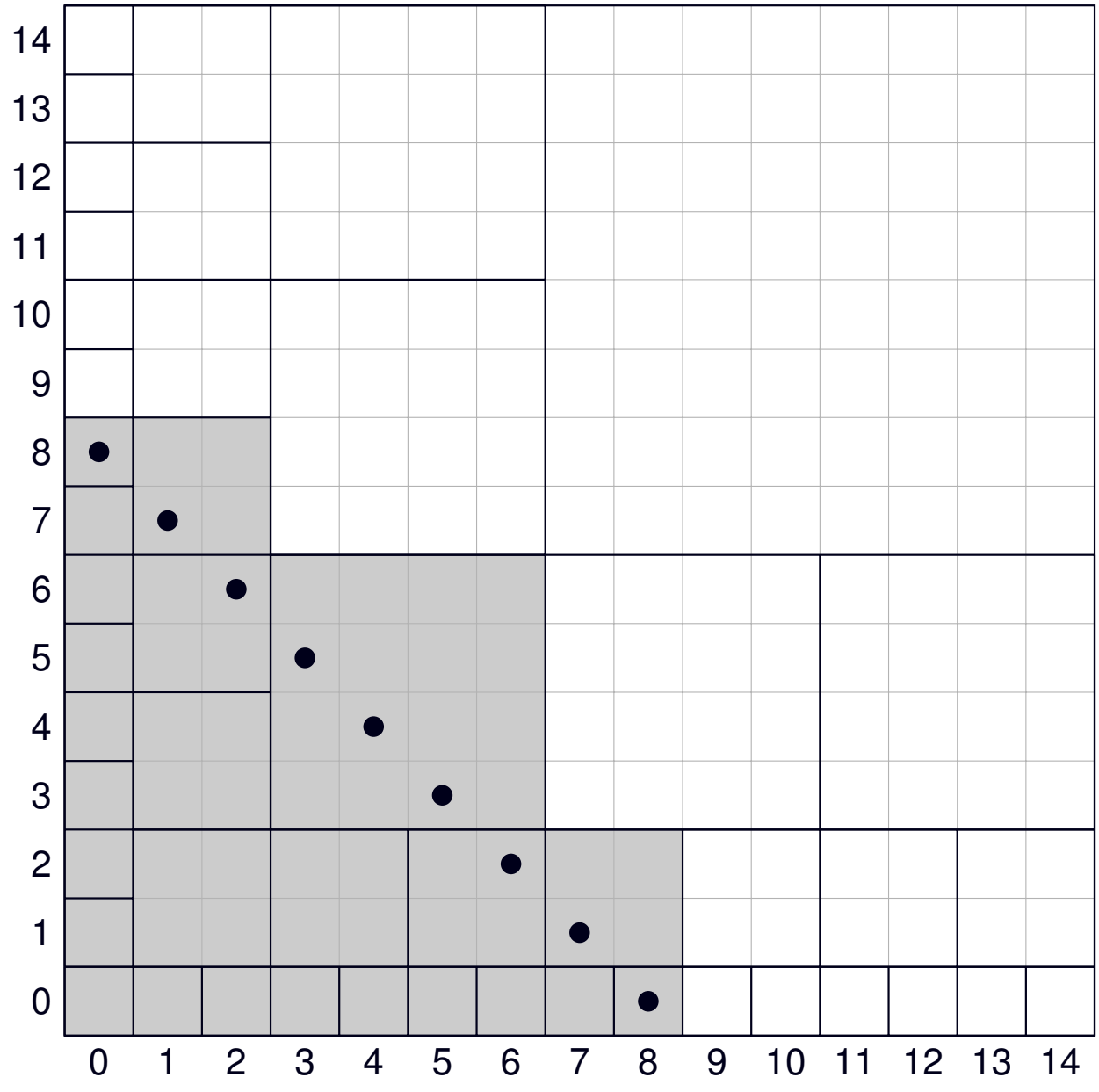
L’arithmétique détendue



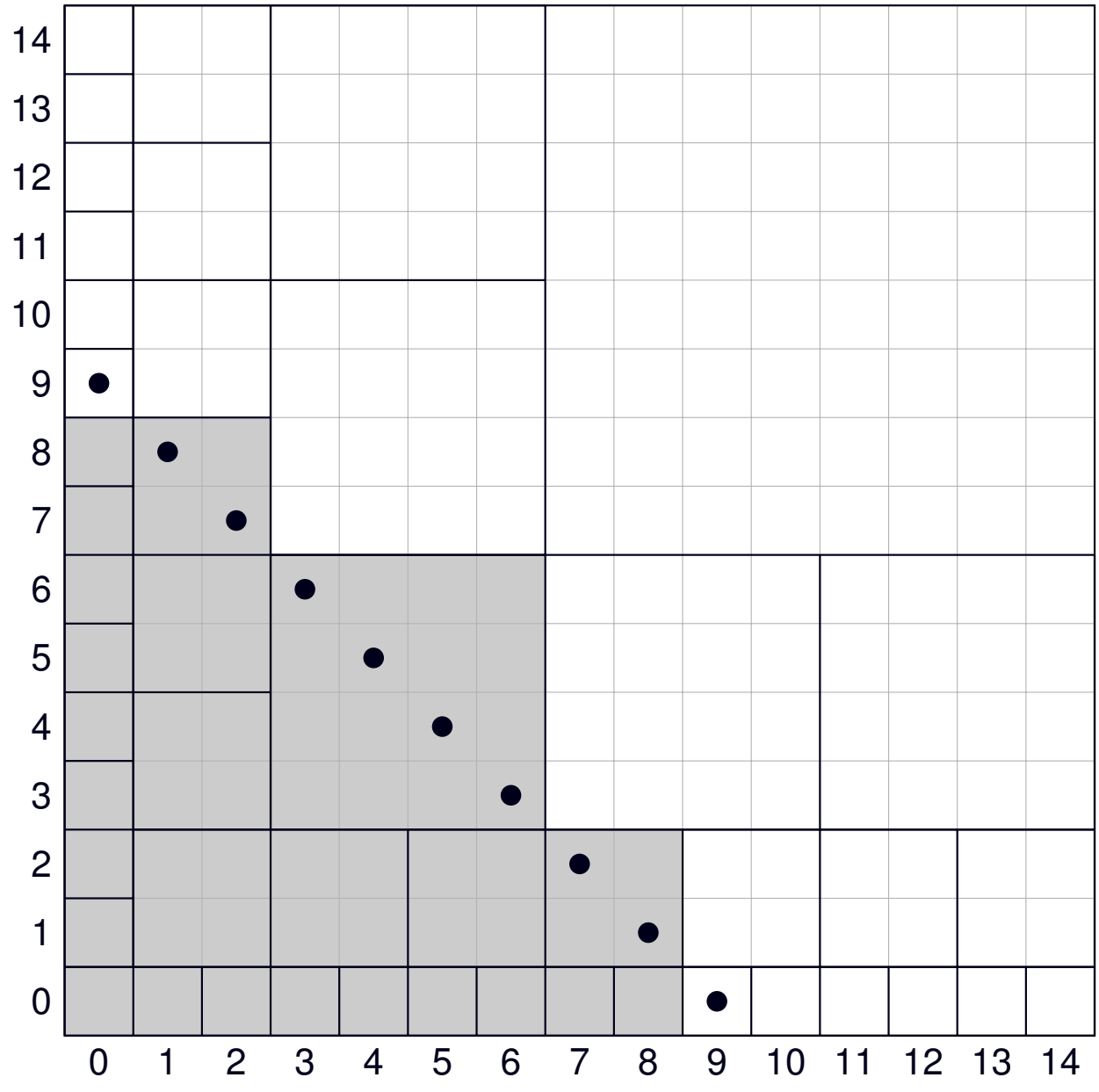
L’arithmétique détendue



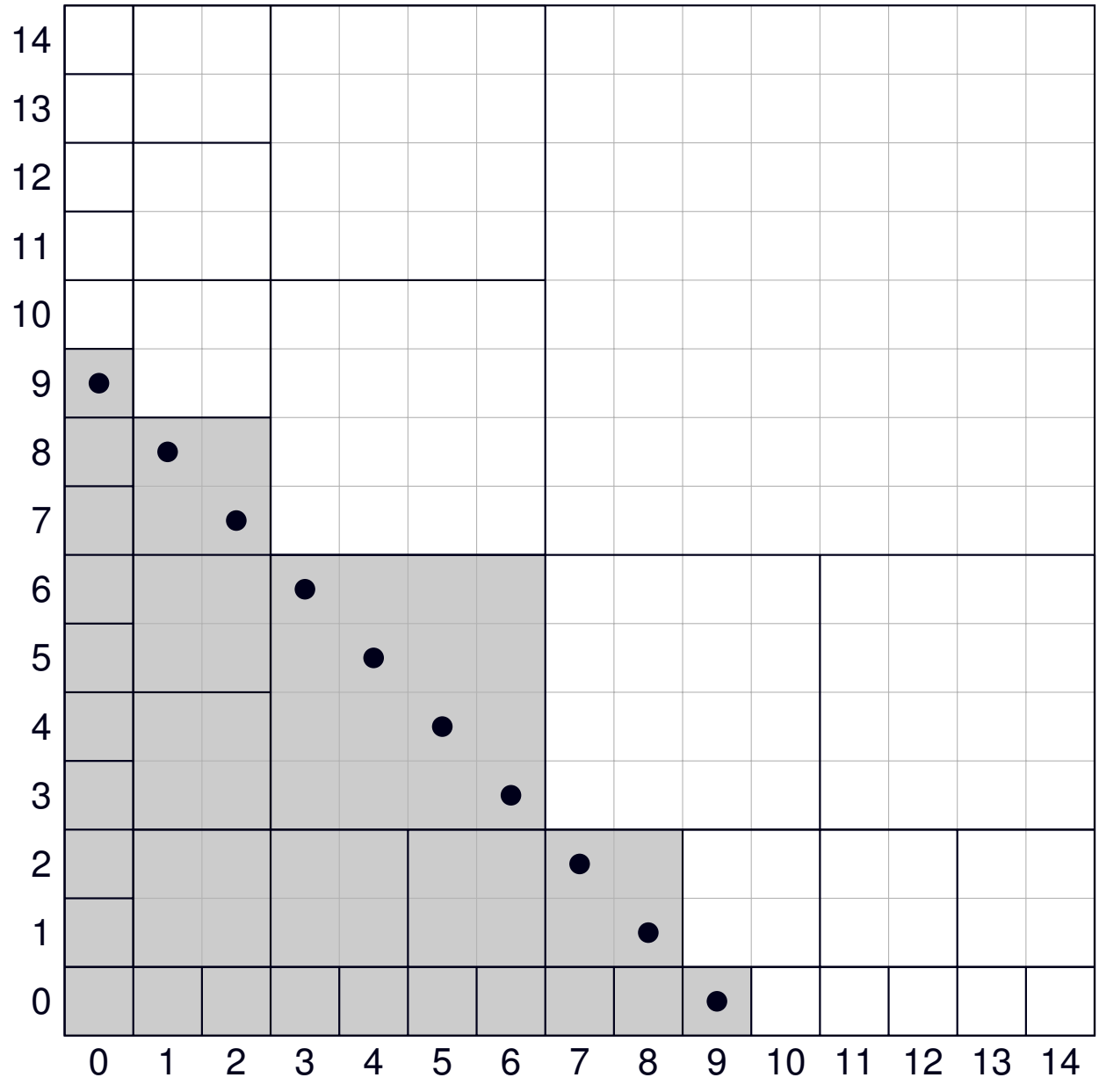
L’arithmétique détendue



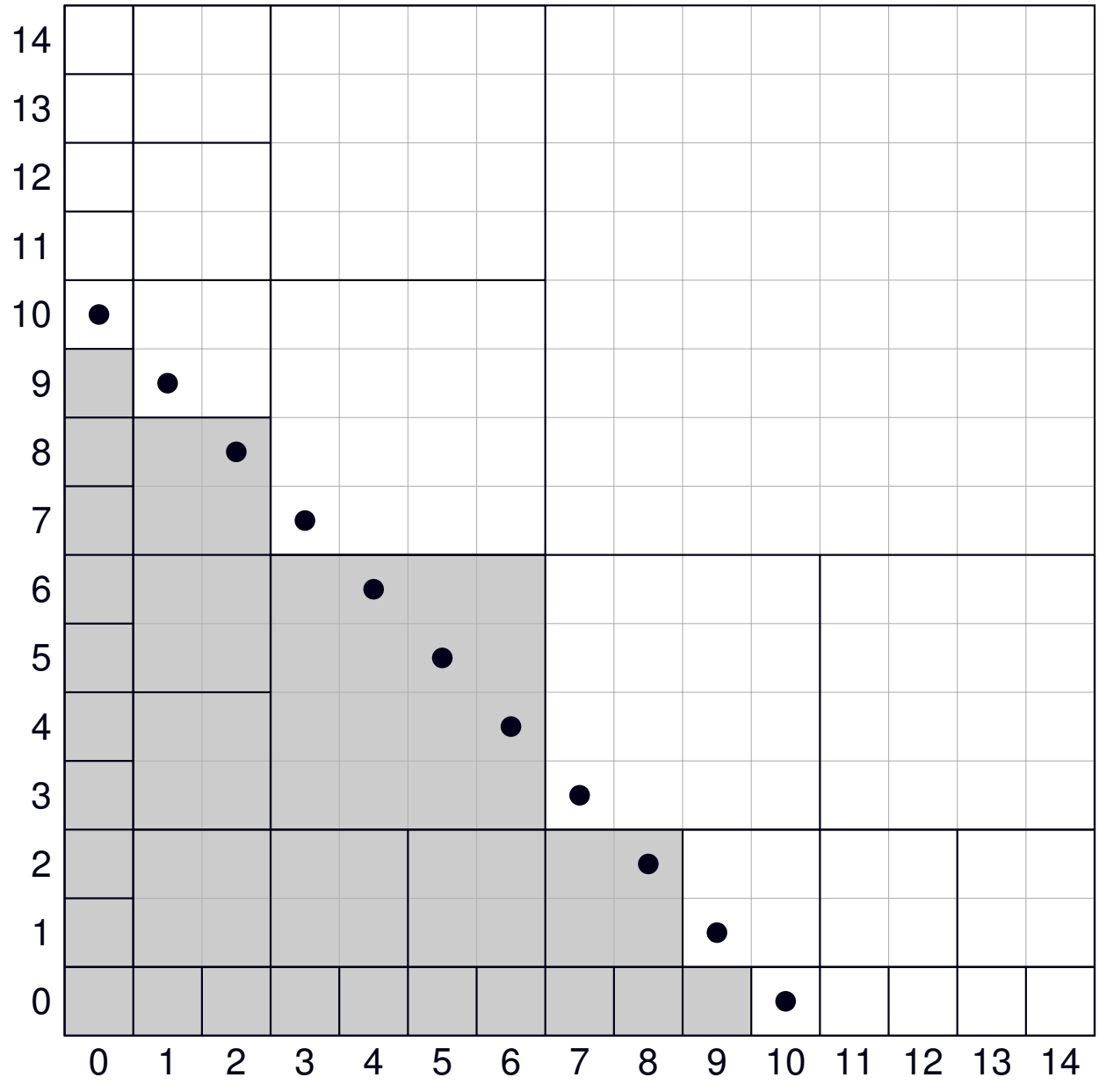
L’arithmétique détendue



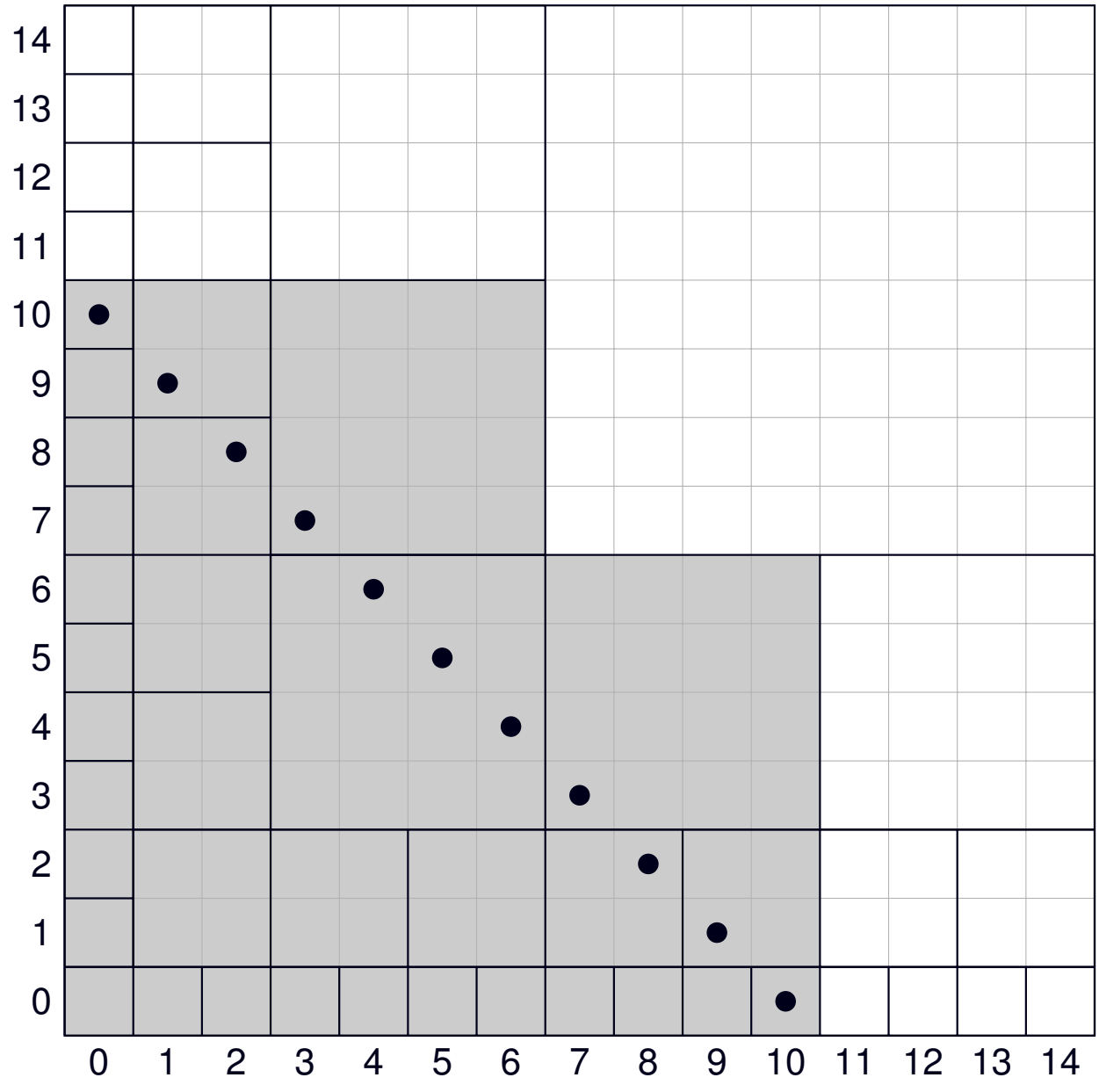
L’arithmétique détendue



L’arithmétique détendue



L’arithmétique détendue



L'arithmétique détendue

```
class x_fois_y(RelaxedPAdicInteger):

    def next(self):
        n = len(self.digits)
        m = n + 2; ℓ = 0; s = 0
        while m > 1:
            # The contribution of the first square of size 2^ℓ
            s += x[2^ℓ - 1, ..., 2^(ℓ+1) - 2]
                 * y[(m-1)*2^ℓ - 1, ..., m*2^ℓ - 2]
            # The contribution of the second square
            if m > 2:
                s += y[2^ℓ - 1, ..., 2^(ℓ+1) - 2]
                     * x[(m-1)*2^ℓ - 1, ..., m*2^ℓ - 2]
            if m is odd: break
            m = m // 2
            ℓ += 1
        s += self.carry
        self.digits[n] = s % p
        self.carry = s // p
```

L’arithmétique flottante

L’arithmétique flottante

Représentation

L'arithmétique flottante

Représentation

- $p^e s$ avec $\frac{p^N - 1}{2} < s \leq \frac{p^N - 1}{2}$ et $\text{PGCD}(s, p) = 1$
- 0
- NaN

Fonction d'arrondi

L'arithmétique flottante

Représentation

- $p^e s$ avec $\dfrac{p^N - 1}{2} < s \leq \dfrac{p^N - 1}{2}$ et $\mathrm{PGCD}(s, p) = 1$
- 0
- NaN

Fonction d'arrondi

$$o : \mathbb{Q}_p \to \mathbb{Q}_p^{\mathrm{FP}} \quad \text{tel que} \quad |x - o(x)| \leq p^{-N}|x|.$$

Opérations

L'arithmétique flottante

Représentation

- $p^e s$ avec $\dfrac{p^N - 1}{2} < s \leq \dfrac{p^N - 1}{2}$ et $\mathrm{PGCD}(s, p) = 1$
- 0
- NaN

Fonction d'arrondi

$$o : \mathbb{Q}_p \to \mathbb{Q}_p^{\mathrm{FP}} \quad \text{tel que} \quad |x - o(x)| \leq p^{-N}|x|.$$

Opérations

$$x +_{\mathrm{FP}} y = o(x + y) \quad ; \quad x -_{\mathrm{FP}} y = o(x - y)$$

$$x \times_{\mathrm{FP}} y = o(xy) \quad ; \quad x \div_{\mathrm{FP}} y = o(\tfrac{x}{y})$$

Quelques points de comparaison

Zélé ou paresseux ?

Quelques points de comparaison

Zélé ou paresseux ?

Utilisation différente

Zélé : précision donnée sur les entrées

Paresseux : précision cible sur la sortie

Quelques points de comparaison

Zélé ou paresseux ?

Utilisation différente

Zélé : précision donnée sur les entrées

Paresseux : précision cible sur la sortie

L'arithmétique paresseuse est ***un peu*** **plus lente**

Quelques points de comparaison

Zélé ou paresseux ?

Utilisation différente

Zélé : précision donnée sur les entrées
Paresseux : précision cible sur la sortie

L'arithmétique paresseuse est ***un peu*** **plus lente**

L'arithmétique paresseuse **requiert plus de mémoire**

Quelques points de comparaison

Zélé ou paresseux ?

Utilisation différente

Zélé : précision donnée sur les entrées

Paresseux : précision cible sur la sortie

L'arithmétique paresseuse est ***un peu*** **plus lente**

L'arithmétique paresseuse **requiert plus de mémoire**

```
def nth_term(n):
    u = 0
    for i in 1,2,...,n: u = f(u)
    return u
```

Quelques points de comparaison

Zélé ou paresseux ?

Utilisation différente

Zélé : précision donnée sur les entrées

Paresseux : précision cible sur la sortie

L'arithmétique paresseuse est ***un peu*** **plus lente**

L'arithmétique paresseuse **requiert plus de mémoire**

```
def nth_term(n):
    u = 0
    for i in 1,2,...,n: u = f(u)
    return u
```

Intervalle ou flottant ?

Quelques points de comparaison

Zélé ou paresseux ?

Utilisation différente

Zélé : précision donnée sur les entrées

Paresseux : précision cible sur la sortie

L'arithmétique paresseuse est ***un peu*** **plus lente**

L'arithmétique paresseuse **requiert plus de mémoire**

```
def nth_term(n):
    u = 0
    for i in 1,2,...,n: u = f(u)
    return u
```

Intervalle ou flottant ?

Résultats **prouvés** en arithmétique d'intervalle

Quelques points de comparaison

Zélé ou paresseux ?

Utilisation différente

Zélé : précision donnée sur les entrées
Paresseux : précision cible sur la sortie

L'arithmétique paresseuse est ***un peu*** **plus lente**

L'arithmétique paresseuse **requiert plus de mémoire**

```
def nth_term(n):
    u = 0
    for i in 1,2,...,n: u = f(u)
    return u
```

Intervalle ou flottant ?

Résultats **prouvés** en arithmétique d'intervalle

Résultats **plus précis** en arithmétique flottante

Exemple : déterminant, polynôme caractéristique

Exemple : déterminant, polynôme caractéristique

$$M = \begin{pmatrix} \ldots 0101110000 & \ldots 0011100000 & \ldots 1011001000 & \ldots 0011000100 \\ \ldots 1101011001 & \ldots 1101000111 & \ldots 0111001010 & \ldots 0101110101 \\ \ldots 0111100011 & \ldots 1011100101 & \ldots 0010100110 & \ldots 1111110111 \\ \ldots 0000111101 & \ldots 1101110011 & \ldots 0011010010 & \ldots 1001100001 \end{pmatrix}$$

Exemple : déterminant, polynôme caractéristique

$$M = \begin{pmatrix} \ldots 0101110000 & \ldots 0011100000 & \ldots 1011001000 & \ldots 0011000100 \\ \ldots 1101011001 & \ldots 1101000111 & \ldots 0111001010 & \ldots 0101110101 \\ \ldots 0111100011 & \ldots 1011100101 & \ldots 0010100110 & \ldots 1111110111 \\ \ldots 0000111101 & \ldots 1101110011 & \ldots 0011010010 & \ldots 1001100001 \end{pmatrix}$$

Arithmétique zélée :

$$\det M = O(2^{10})$$

Exemple : déterminant, polynôme caractéristique

$$M = \begin{pmatrix} \ldots 0101110000 & \ldots 0011100000 & \ldots 1011001000 & \ldots 0011000100 \\ \ldots 1101011001 & \ldots 1101000111 & \ldots 0111001010 & \ldots 0101110101 \\ \ldots 0111100011 & \ldots 1011100101 & \ldots 0010100110 & \ldots 1111110111 \\ \ldots 0000111101 & \ldots 1101110011 & \ldots 0011010010 & \ldots 1001100001 \end{pmatrix}$$

Arithmétique zélée :

$$\det M = O(2^{10})$$

Arithmétique flottante :

$$\det M = 2^{10} \times \ldots 00010\mathbf{01101}$$

Exemple : déterminant, polynôme caractéristique

$$M = \begin{pmatrix} \ldots 0101110000 & \ldots 0011100000 & \ldots 1011001000 & \ldots 0011000100 \\ \ldots 1101011001 & \ldots 1101000111 & \ldots 0111001010 & \ldots 0101110101 \\ \ldots 0111100011 & \ldots 1011100101 & \ldots 0010100110 & \ldots 1111110111 \\ \ldots 0000111101 & \ldots 1101110011 & \ldots 0011010010 & \ldots 1001100001 \end{pmatrix}$$

Arithmétique zélée :

$$\det M = O(2^{10})$$

Arithmétique flottante :

$$\det M = 2^{10} \times \ldots 00010\,01101$$

Arithmétique zélée :

$$\begin{aligned} \chi_M(X) = X^4 + & \quad (\ldots 0001000010)\, X^3 + & (\ldots 1000101100)\, X^2 \\ + & \quad (\ldots 0011100000)\, X + & (\ldots 0000000000) \end{aligned}$$

Exemple : déterminant, polynôme caractéristique

$$M = \begin{pmatrix} \ldots 0101110000 & \ldots 0011100000 & \ldots 1011001000 & \ldots 0011000100 \\ \ldots 1101011001 & \ldots 1101000111 & \ldots 0111001010 & \ldots 0101110101 \\ \ldots 0111100011 & \ldots 1011100101 & \ldots 0010100110 & \ldots 1111110111 \\ \ldots 0000111101 & \ldots 1101110011 & \ldots 0011010010 & \ldots 1001100001 \end{pmatrix}$$

Arithmétique zélée :

$$\det M = O(2^{10})$$

Arithmétique flottante :

$$\det M = 2^{10} \times \ldots 00010\mathbf{01101}$$

Arithmétique zélée :

$$\begin{aligned} \chi_M(X) = X^4 + & \quad (\ldots 0001000010)\, X^3 + \quad (\ldots 1000101100)\, X^2 \\ + & \quad (\ldots 0011100000)\, X + \quad (\ldots 0000000000) \end{aligned}$$

Arithmétique flottante :

$$\begin{aligned} \chi_M(X) = X^4 + & \quad (\ldots 0\mathbf{0001000010})\, X^3 + \quad (\ldots 11\mathbf{1000101100})\, X^2 \\ + & \, (\ldots 110\mathbf{100011100000})\, X + (2^{10} \times \ldots 00010\mathbf{01101}) \end{aligned}$$

Exemple : factorisation LU

Exemple : factorisation LU

$$M = \begin{pmatrix} \ldots 0101110000 & \ldots 0011100000 & \ldots 1011001000 & \ldots 0011000100 \\ \ldots 1101011001 & \ldots 1101000111 & \ldots 0111001010 & \ldots 0101110101 \\ \ldots 0111100011 & \ldots 1011100101 & \ldots 0010100110 & \ldots 1111110111 \\ \ldots 0000111101 & \ldots 1101110011 & \ldots 0011010010 & \ldots 1001100001 \end{pmatrix}$$

Exemple : factorisation LU

$$M = \begin{pmatrix} \ldots 0101110000 & \ldots 0011100000 & \ldots 1011001000 & \ldots 0011000100 \\ \ldots 1101011001 & \ldots 1101000111 & \ldots 0111001010 & \ldots 0101110101 \\ \ldots 0111100011 & \ldots 1011100101 & \ldots 0010100110 & \ldots 1111110111 \\ \ldots 0000111101 & \ldots 1101110011 & \ldots 0011010010 & \ldots 1001100001 \end{pmatrix}$$

Arithmétique zélée :

$$L = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2^{-4} \times \ldots 001111 & 1 & 0 & 0 \\ 2^{-4} \times \ldots 010101 & \ldots 100011 & 1 & 0 \\ 2^{-4} \times \ldots 001011 & \ldots 010101 & \ldots 110 & 1 \end{pmatrix}$$

Exemple : factorisation LU

$$M = \begin{pmatrix} \ldots 0101110000 & \ldots 0011100000 & \ldots 1011001000 & \ldots 0011000100 \\ \ldots 1101011001 & \ldots 1101000111 & \ldots 0111001010 & \ldots 0101110101 \\ \ldots 0111100011 & \ldots 1011100101 & \ldots 0010100110 & \ldots 1111110111 \\ \ldots 0000111101 & \ldots 1101110011 & \ldots 0011010010 & \ldots 1001100001 \end{pmatrix}$$

Arithmétique zélée :

$$L = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2^{-4} \times \ldots 001111 & 1 & 0 & 0 \\ 2^{-4} \times \ldots 010101 & \ldots 100011 & 1 & 0 \\ 2^{-4} \times \ldots 001011 & \ldots 010101 & \ldots 110 & 1 \end{pmatrix}$$

Arithmétique flottante :

$$L = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2^{-4} \times \ldots 1010001111 & 1 & 0 & 0 \\ 2^{-4} \times \ldots 0110010101 & \ldots 0011100011 & 1 & 0 \\ 2^{-4} \times \ldots 0101001011 & \ldots 0111010101 & 00010110110 & 1 \end{pmatrix}$$

Exemple : coefficients de Bézout

Exemple : coefficients de Bézout

$$\begin{aligned} P = X^4 &+ (\ldots 1101111111)\, X^3 + (\ldots 0011110011)\, X^2 \\ &+ (\ldots 1001001100)\, X \;+ (\ldots 0010111010) \end{aligned}$$

$$\begin{aligned} Q = X^4 &+ (\ldots 0101001011)\, X^3 + (\ldots 0111001111)\, X^2 \\ &+ (\ldots 0100010000)\, X \;+ (\ldots 1101000111) \end{aligned}$$

Exemple : coefficients de Bézout

$$\begin{aligned} P = X^4 &+ (\ldots 1101111111)\, X^3 + (\ldots 0011110011)\, X^2 \\ &+ (\ldots 1001001100)\, X \;+ (\ldots 0010111010) \end{aligned}$$

$$\begin{aligned} Q = X^4 &+ (\ldots 0101001011)\, X^3 + (\ldots 0111001111)\, X^2 \\ &+ (\ldots 0100010000)\, X \;+ (\ldots 1101000111) \end{aligned}$$

Arithmétique zélée :

$$\begin{aligned} U = \quad & (\ldots 101100)\, X^3 + \quad (\ldots 101100)\, X^2 \\ + \quad & (\ldots 100)\, X \;+ \quad (\ldots 1011) \end{aligned}$$

$$\begin{aligned} V = \quad & (\ldots 010100)\, X^3 + \quad (\ldots 100100)\, X^2 \\ + \quad & (\ldots 100)\, X \;+ \quad (\ldots 101) \end{aligned}$$

Exemple : coefficients de Bézout

$$P = X^4 + (\ldots 1101111111)\, X^3 + (\ldots 0011110011)\, X^2 + (\ldots 1001001100)\, X + (\ldots 0010111010)$$

$$Q = X^4 + (\ldots 0101001011)\, X^3 + (\ldots 0111001111)\, X^2 + (\ldots 0100010000)\, X + (\ldots 1101000111)$$

Arithmétique zélée :

$$U = (\ldots 101100)\, X^3 + (\ldots 101100)\, X^2 + (\ldots 100)\, X + (\ldots 1011)$$

$$V = (\ldots 010100)\, X^3 + (\ldots 100100)\, X^2 + (\ldots 100)\, X + (\ldots 101)$$

Arithmétique flottante :

$$U = (\ldots 101011101100)\, X^3 + (\ldots 111100101100)\, X^2 + (\ldots 100000110100)\, X + (\ldots 01100011011)$$

$$V = (\ldots 010100010100)\, X^3 + (\ldots 001011100100)\, X^2 + (\ldots 000100111100)\, X + (\ldots 11111100101)$$

Exemple : évaluation et interpolation

Exemple : évaluation et interpolation

$$
\begin{aligned}
P = &(\ldots 01111001110)\, X^8 + (\ldots 0101010001)\, X^7 + (\ldots 1000001100)\, X^6 \\
&+ (\ldots 1010001101)\, X^5 + (\ldots 1111000100)\, X^4 + (\ldots 0011101101)\, X^3 \\
&+ (\ldots 1010010111)\, X^2 + (\ldots 0011011010)\, X \; + (\ldots 0001011110)
\end{aligned}
$$

Exemple : évaluation et interpolation

$$\begin{aligned} P = &(\ldots 01111001110)\, X^8 + (\ldots 0101010001)\, X^7 + (\ldots 1000001100)\, X^6 \\ &+ (\ldots 1010001101)\, X^5 + (\ldots 1111000100)\, X^4 + (\ldots 0011101101)\, X^3 \\ &+ (\ldots 1010010111)\, X^2 + (\ldots 0011011010)\, X + (\ldots 0001011110) \end{aligned}$$

Arithmétique zélée :

$$\begin{aligned} &(\ldots 110)\, X^8 + &&(\ldots 001)\, X^7 + &&(\ldots 100)\, X^6 \\ + \quad &(\ldots 101)\, X^5 + &&(\ldots 100)\, X^4 + &&(\ldots 1101)\, X^3 \\ + \quad &(\ldots 10111)\, X^2 + &&(\ldots 1011010)\, X + &&(\ldots 0001011110) \end{aligned}$$

Exemple : évaluation et interpolation

$$\begin{aligned} P = &(\ldots 01111001110)\, X^8 + (\ldots 0101010001)\, X^7 + (\ldots 1000001100)\, X^6 \\ &+ (\ldots 1010001101)\, X^5 + (\ldots 1111000100)\, X^4 + (\ldots 0011101101)\, X^3 \\ &+ (\ldots 1010010111)\, X^2 + (\ldots 0011011010)\, X + (\ldots 0001011110) \end{aligned}$$

Arithmétique zélée :

$$\begin{aligned} &(\ldots 110)\, X^8 + &&(\ldots 001)\, X^7 + &&(\ldots 100)\, X^6 \\ + &(\ldots 101)\, X^5 + &&(\ldots 100)\, X^4 + &&(\ldots 1101)\, X^3 \\ + &(\ldots 10111)\, X^2 + &&(\ldots 1011010)\, X + &&(\ldots 0001011110) \end{aligned}$$

Arithmétique flottante :

$$\begin{aligned} &(\ldots 00001001110)\, X^8 + &&(\ldots 1011010001)\, X^7 + &&(\ldots 001010001100)\, X^6 \\ + &(\ldots 0010001101)\, X^5 + &&(\ldots 000011000100)\, X^4 + &&(\ldots 010111011101)\, X^3 \\ + &(\ldots 0010010111)\, X^2 + &&(\ldots 11011011010)\, X + &&(\ldots 00001011110) \end{aligned}$$

Exemple : évaluation et interpolation

$$
\begin{aligned}
P = {} & (\ldots 0101101001)\, X^{19} + (\ldots 1101000011)\, X^{18} + (\ldots 0011001110)\, X^{17} + (\ldots 1001011010)\, X^{16} \\
& + (\ldots 0011100111)\, X^{15} + (\ldots 0110101110)\, X^{14} + (\ldots 0111111001)\, X^{13} + (\ldots 1011010111)\, X^{12} \\
& + (\ldots 0100000100)\, X^{11} + (\ldots 0000110000)\, X^{10} + (\ldots 1110101010)\, X^{9} + (\ldots 1111101100)\, X^{8} \\
& + (\ldots 0100010001)\, X^{7} + (\ldots 0101010000)\, X^{6} + (\ldots 0111101111)\, X^{5} + (\ldots 1100010011)\, X^{4} \\
& + (\ldots 0100000001)\, X^{3} + (\ldots 1000010010)\, X^{2} + (\ldots 0000100000)\, X + (\ldots 0001111110)
\end{aligned}
$$

Arithmétique zélée :

$$
\begin{aligned}
& O(2^{-6})\, X^{19} + && O(2^{-6})\, X^{18} + && O(2^{-6})\, X^{17} \\
+ \; & O(2^{-5})\, X^{16} + && O(2^{-6})\, X^{15} + && O(2^{-6})\, X^{14} \\
+ \; & O(2^{-6})\, X^{13} + && O(2^{-5})\, X^{12} + && O(2^{-6})\, X^{11} \\
+ \; & O(2^{-6})\, X^{10} + && O(2^{-6})\, X^{9} + && O(2^{-5})\, X^{8} \\
+ \; & O(2^{-4})\, X^{7} + && O(2^{-3})\, X^{6} + && O(2^{-2})\, X^{5} \\
+ \; & O(2^{-1})\, X^{4} + && (\ldots 1)\, X^{3} + && (\ldots 010)\, X^{2} \\
+ \; & (\ldots 100000)\, X + && (\ldots 0001111110) &&
\end{aligned}
$$

Arithmétique flottante :

$$
\begin{aligned}
& (2^{-3} \times \ldots 1110011011)\, X^{19} + (2^{-5} \times \ldots 0000000011)\, X^{18} + (2^{-3} \times \ldots 0001011111)\, X^{17} \\
+ \; & (2^{-5} \times \ldots 1100111101)\, X^{16} + && (\ldots 11111100110)\, X^{15} + (2^{-4} \times \ldots 0110100011)\, X^{14} \\
+ \; & (2^{-2} \times \ldots 0000010011)\, X^{13} + (2^{-4} \times \ldots 1010001101)\, X^{12} + (2^{-3} \times \ldots 0010000011)\, X^{11} \\
+ \; & (2^{-5} \times \ldots 0100101111)\, X^{10} + (2^{-3} \times \ldots 0000110011)\, X^{9} + (2^{-5} \times \ldots 1010101001)\, X^{8} \\
+ \; & (2^{-2} \times \ldots 0010000101)\, X^{7} + (2^{-2} \times \ldots 1101100111)\, X^{6} + && (\ldots 1101101111)\, X^{5} \\
+ \; & (2^{-1} \times \ldots 0011100111)\, X^{4} + && (\ldots 0101110101)\, X^{3} + && (\ldots 1101110101 0)\, X^{2} \\
+ \; & (\ldots 0000000011 00000)\, X + && (\ldots 0000111111 0) &&
\end{aligned}
$$

Arithmétique zélée et itération de Newton

Arithmétique zélée et itération de Newton

Objectif

Calcul de $\sqrt{\ldots 11110010010000111001}$

Arithmétique zélée et itération de Newton

Objectif

Calcul de $\sqrt{\ldots 11110010010000111001}$

Schéma de Newton

$$x_0 = 1 \quad ; \quad x_{i+1} = \frac{1}{2}\left(x_i + \frac{c}{x_i}\right)$$

Arithmétique zélée et itération de Newton

Objectif

Calcul de $\sqrt{\ldots 11110010010000111001}$

Schéma de Newton

$$x_0 = 1 \quad ; \quad x_{i+1} = \frac{1}{2}\left(x_i + \frac{c}{x_i}\right)$$

Résultats

Arithmétique zélée et itération de Newton

Objectif

Calcul de $\sqrt{\ldots 11110010010000111001}$

Schéma de Newton

$$x_0 = 1 \quad ; \quad x_{i+1} = \frac{1}{2}\left(x_i + \frac{c}{x_i}\right)$$

Résultats

$$\begin{aligned}
x_1 &: \quad \ldots 11110010010000111101 \\
x_2 &: \quad \ldots 00111010001111010101 \\
x_3 &: \quad \ldots 10111010001010101 \\
x_4 &: \quad \ldots 0111010001010101 \\
x_5 &: \quad \ldots 111010001010101 \\
x_6 &: \quad \ldots 11010001010101
\end{aligned}$$

Arithmétique zélée et itération de Newton

Objectif

Calcul de $\sqrt{\ldots 11110010010000111001}$

Schéma de Newton

$$x_0 = 1 \quad ; \quad x_{i+1} = \frac{1}{2}\left(x_i + \frac{c}{x_i}\right)$$

Résultats

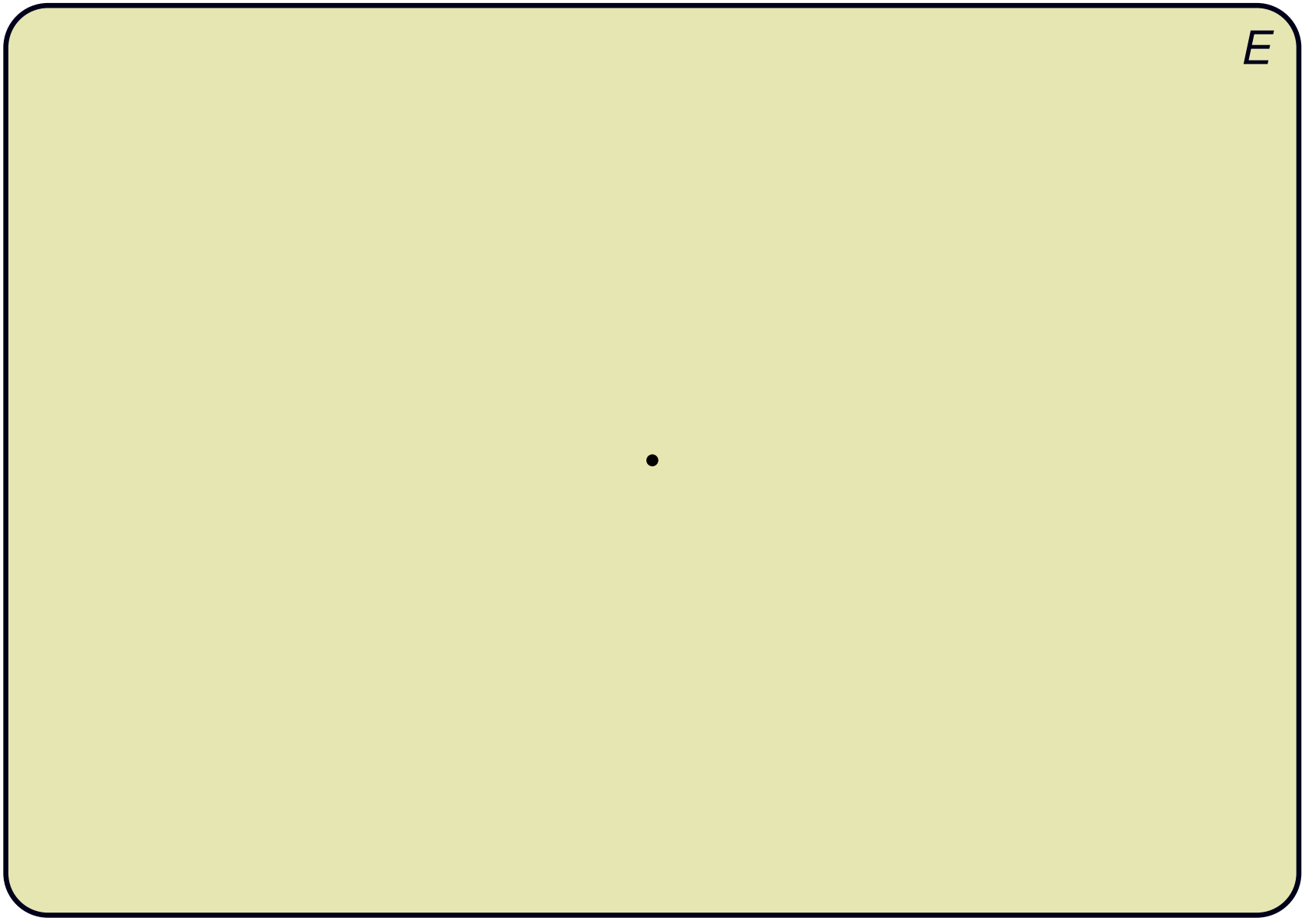
$$\begin{aligned}
x_1 &: \quad \ldots 00000000000000000101 \\
x_2 &: \quad \ldots 00000000000000010101 \\
x_3 &: \quad \ldots 00000000000001010101 \\
x_4 &: \quad \ldots 00010111101000101010 1 \\
x_5 &: \quad \ldots 10101111010001010101 \\
x_6 &: \quad \ldots 10101111010001010101
\end{aligned}$$

Troisième partie

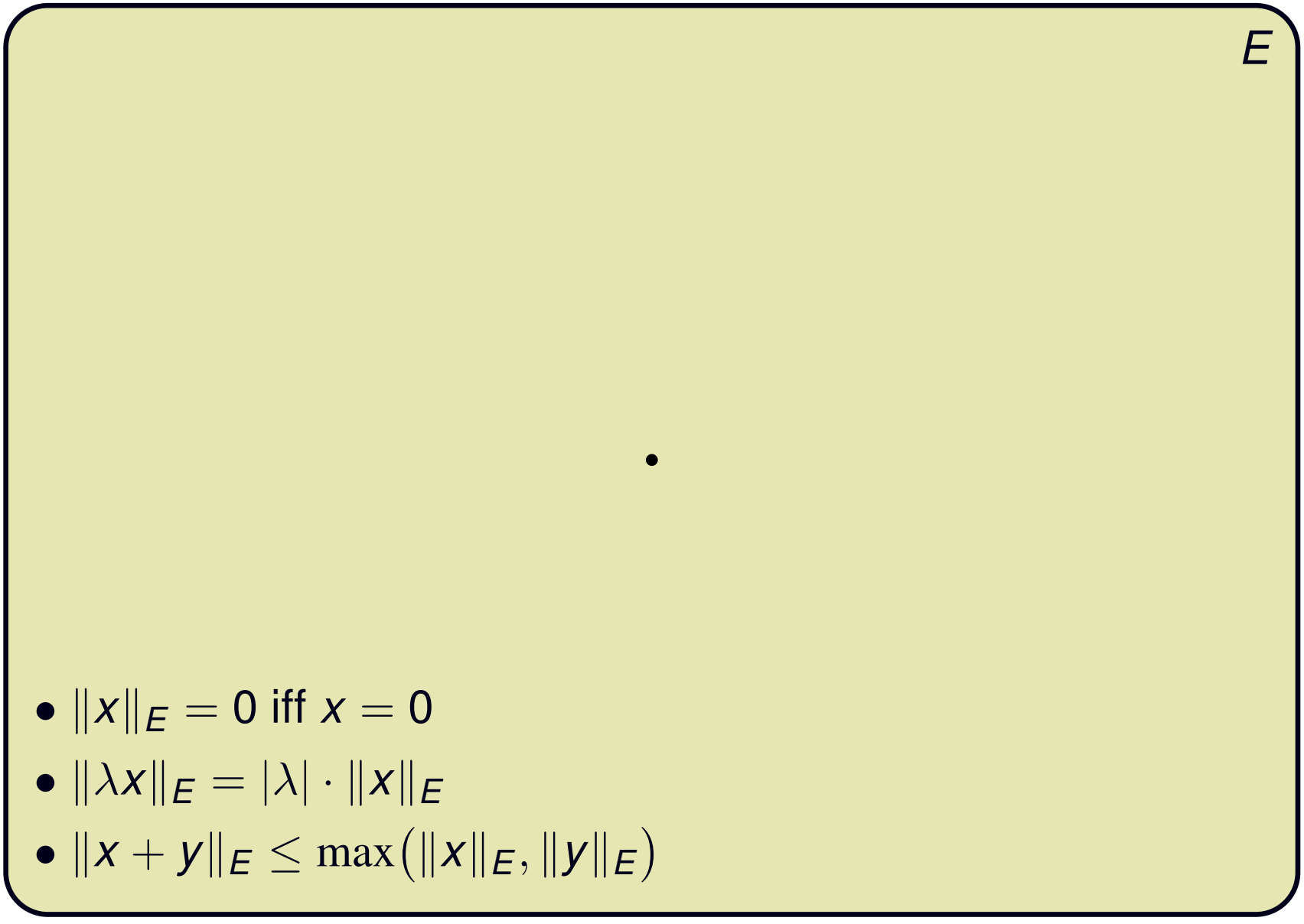
Suivi de la précision p-adique

Réseaux dans les espaces vectoriels p-adiques

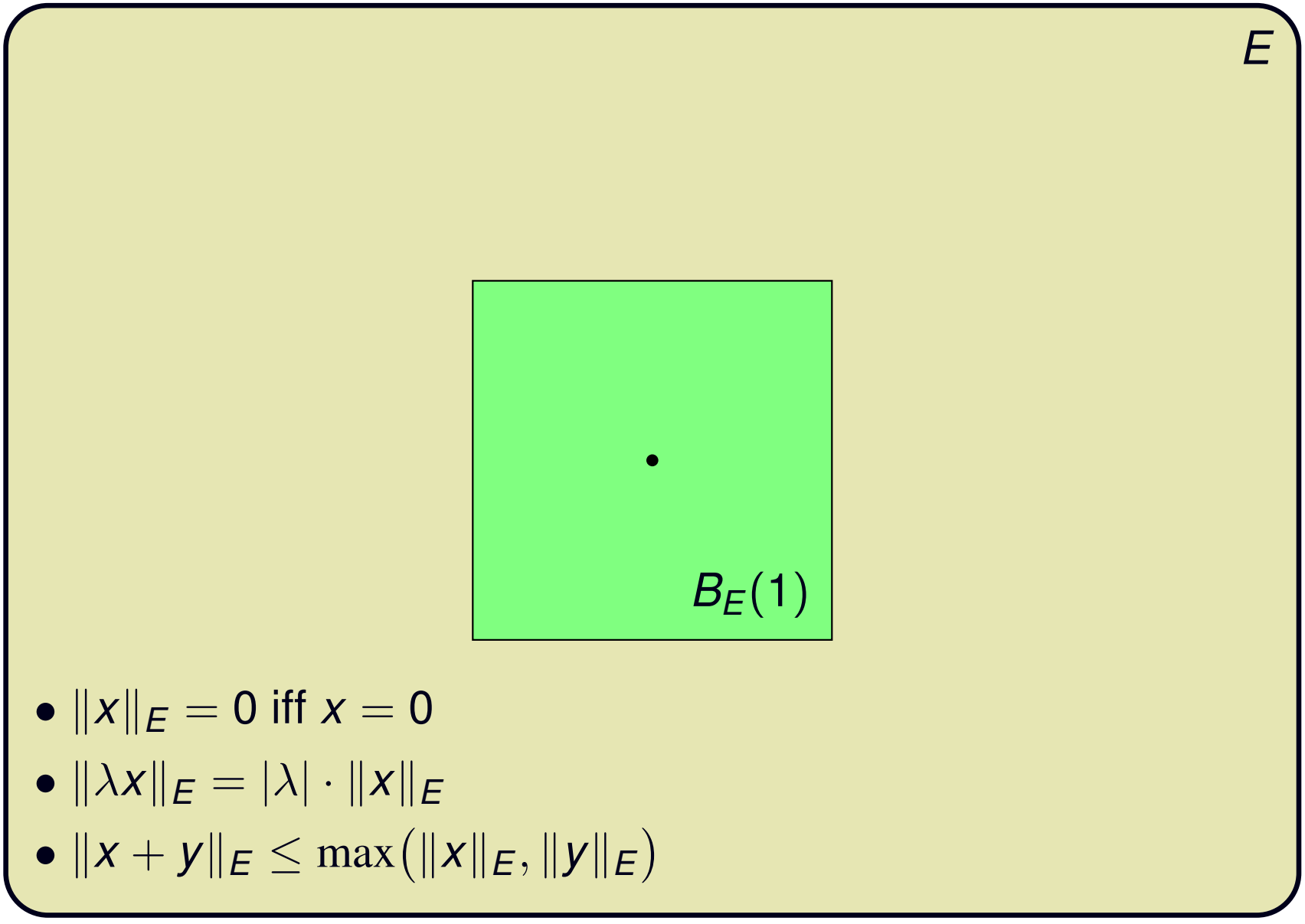
Réseaux dans les espaces vectoriels *p*-adiques



Réseaux dans les espaces vectoriels p-adiques

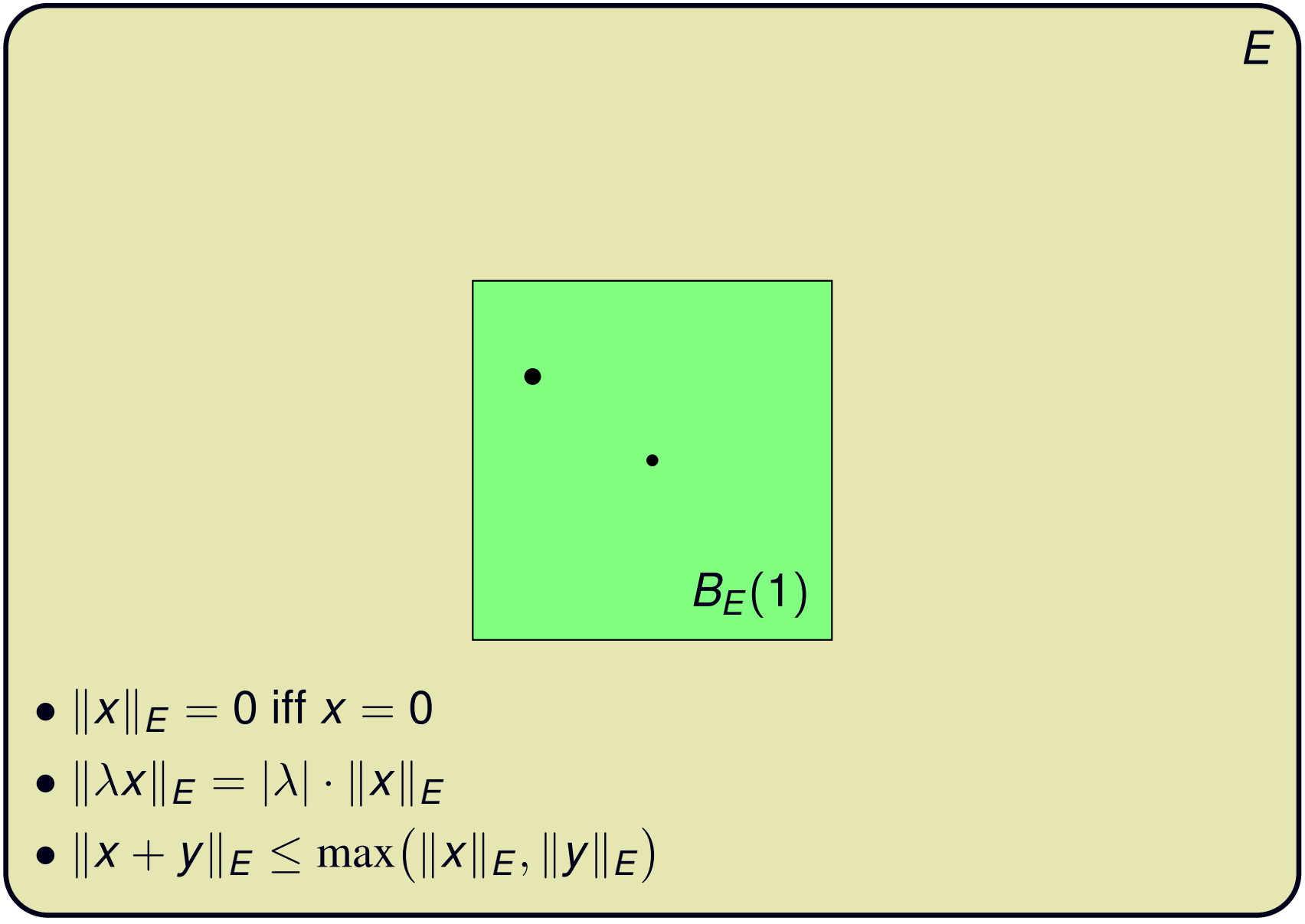


Réseaux dans les espaces vectoriels p-adiques



- $\|x\|_E = 0$ iff $x = 0$
- $\|\lambda x\|_E = |\lambda| \cdot \|x\|_E$
- $\|x + y\|_E \leq \max\big(\|x\|_E, \|y\|_E\big)$

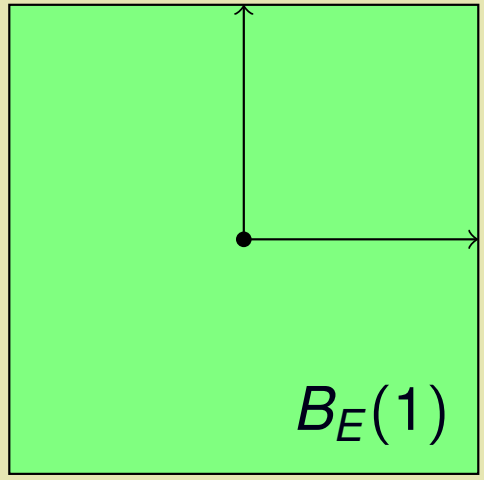
Réseaux dans les espaces vectoriels p-adiques



- $\|x\|_E = 0$ iff $x = 0$
- $\|\lambda x\|_E = |\lambda| \cdot \|x\|_E$
- $\|x + y\|_E \leq \max\big(\|x\|_E, \|y\|_E\big)$

Réseaux dans les espaces vectoriels p-adiques

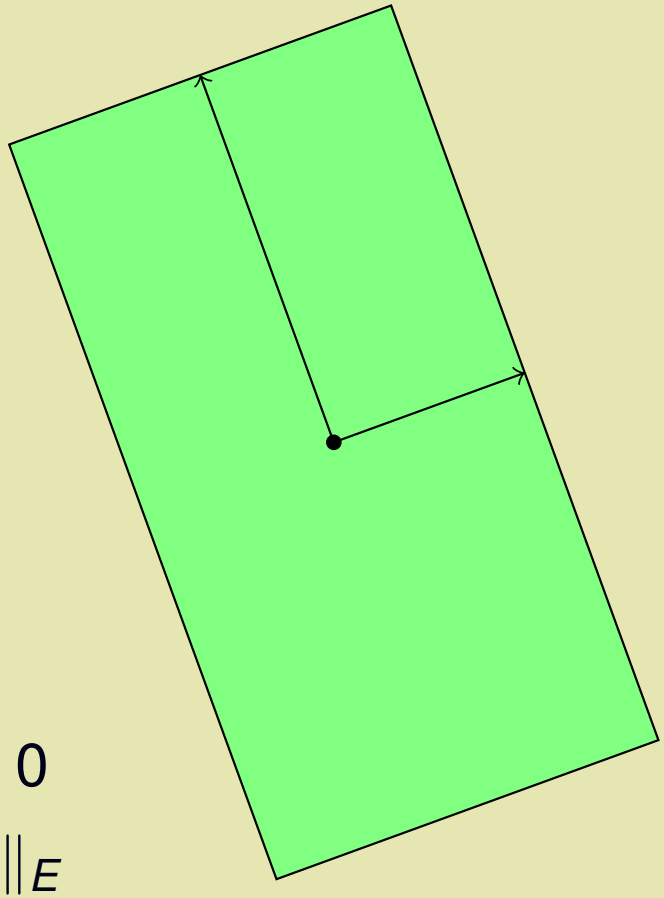
E



- $\|x\|_E = 0$ iff $x = 0$
- $\|\lambda x\|_E = |\lambda| \cdot \|x\|_E$
- $\|x + y\|_E \leq \max\big(\|x\|_E, \|y\|_E\big)$

Réseaux dans les espaces vectoriels p-adiques

E



- $\|x\|_E = 0$ iff $x = 0$
- $\|\lambda x\|_E = |\lambda| \cdot \|x\|_E$
- $\|x + y\|_E \leq \max\big(\|x\|_E, \|y\|_E\big)$

Manipulation de réseaux

Manipulation de réseaux

Réduction de Hermite

Manipulation de réseaux

Réduction de Hermite

$$\begin{pmatrix} \ldots 0101110000 & \ldots 0011100000 & \ldots 1011001000 & \ldots 0011000100 \\ \ldots 1101011001 & \ldots 1101000111 & \ldots 0111001010 & \ldots 0101110101 \\ \ldots 0111100011 & \ldots 1011100101 & \ldots 0010100110 & \ldots 1111110111 \\ \ldots 0000111101 & \ldots 1101110011 & \ldots 0011010010 & \ldots 1001100001 \end{pmatrix}$$

Manipulation de réseaux

Réduction de Hermite

$$\begin{pmatrix} \ldots 1101011001 & \ldots 1101000111 & \ldots 0111001010 & \ldots 0101110101 \\ \ldots 0101110000 & \ldots 0011100000 & \ldots 1011001000 & \ldots 0011000100 \\ \ldots 0111100011 & \ldots 1011100101 & \ldots 0010100110 & \ldots 1111110111 \\ \ldots 0000111101 & \ldots 1101110011 & \ldots 0011010010 & \ldots 1001100001 \end{pmatrix}$$

Manipulation de réseaux

Réduction de Hermite

$$\begin{pmatrix} 1 & \ldots 1110011111 & \ldots 0011011010 & \ldots 1101111101 \\ \ldots 0101110000 & \ldots 0011100000 & \ldots 1011001000 & \ldots 0011000100 \\ \ldots 0111100011 & \ldots 1011100101 & \ldots 0010100110 & \ldots 1111110111 \\ \ldots 0000111101 & \ldots 1101110011 & \ldots 0011010010 & \ldots 1001100001 \end{pmatrix}$$

Manipulation de réseaux

Réduction de Hermite

$$\begin{pmatrix} 1 & \ldots 1110011111 & \ldots 0011011010 & \ldots 1101111101 \\ 0 & \ldots 0001010000 & \ldots 0101101000 & \ldots 0100010100 \\ 0 & \ldots 0111101000 & \ldots 0101011000 & \ldots 1100100000 \\ 0 & \ldots 1010010000 & \ldots 0011100000 & \ldots 0011011000 \end{pmatrix}$$

Manipulation de réseaux

Réduction de Hermite

$$\begin{pmatrix} 1 & \ldots 1110011111 & \ldots 0011011010 & \ldots 1101111101 \\ 0 & \ldots 0111101000 & \ldots 0101011000 & \ldots 1100100000 \\ 0 & \ldots 0001010000 & \ldots 0101101000 & \ldots 0100010100 \\ 0 & \ldots 1010010000 & \ldots 0011100000 & \ldots 0011011000 \end{pmatrix}$$

Manipulation de réseaux

Réduction de Hermite

$$\begin{pmatrix} 1 & \ldots 1110011111 & \ldots 0011011010 & \ldots 1101111101 \\ 0 & 2^3 & \ldots 0000111000 & \ldots 0110100000 \\ 0 & \ldots 0001010000 & \ldots 0101101000 & \ldots 0100010100 \\ 0 & \ldots 1010010000 & \ldots 0011100000 & \ldots 0011011000 \end{pmatrix}$$

Manipulation de réseaux

Réduction de Hermite

$$\begin{pmatrix} 1 & \dots 1110011111 & \dots 0011011010 & \dots 1101111101 \\ 0 & 2^3 & \dots 0000111000 & \dots 0110100000 \\ 0 & 0 & \dots 1100111000 & \dots 0011010100 \\ 0 & 0 & \dots 1011110000 & \dots 0001011000 \end{pmatrix}$$

Manipulation de réseaux

Réduction de Hermite

$$\begin{pmatrix} 1 & \ldots 1110011111 & \ldots 0011011010 & \ldots 1101111101 \\ 0 & 2^3 & \ldots 0000111000 & \ldots 0110100000 \\ 0 & 0 & 2^3 & \ldots 000001100 \\ 0 & 0 & \ldots 1011110000 & \ldots 0001011000 \end{pmatrix}$$

Manipulation de réseaux

Réduction de Hermite

$$\begin{pmatrix} 1 & \dots 1110011111 & \dots 0011011010 & \dots 1101111101 \\ 0 & 2^3 & \dots 0000111000 & \dots 0110100000 \\ 0 & 0 & 2^3 & \dots 000001100 \\ 0 & 0 & 0 & \dots 111110000 \end{pmatrix}$$

Manipulation de réseaux

Réduction de Hermite

$$\begin{pmatrix} 1 & \dots 1110011111 & \dots 0011011010 & \dots 1101111101 \\ 0 & 2^3 & \dots 0000111000 & \dots 0110100000 \\ 0 & 0 & 2^3 & \dots 000001100 \\ 0 & 0 & 0 & 2^4 \end{pmatrix}$$

Manipulation de réseaux

Réduction de Hermite

$$\begin{pmatrix} 1 & 7 & \dots 1110110010 & \dots 0010011101 \\ 0 & 2^3 & \dots 0000111000 & \dots 0110100000 \\ 0 & 0 & 2^3 & \dots 000001100 \\ 0 & 0 & 0 & 2^4 \end{pmatrix}$$

Manipulation de réseaux

Réduction de Hermite

$$\begin{pmatrix} 1 & 7 & 2 & \dots 1100010101 \\ 0 & 2^3 & \dots 0000111000 & \dots 0110100000 \\ 0 & 0 & 2^3 & \dots 000001100 \\ 0 & 0 & 0 & 2^4 \end{pmatrix}$$

Manipulation de réseaux

Réduction de Hermite

$$\begin{pmatrix} 1 & 7 & 2 & \dots 1100010101 \\ 0 & 2^3 & 0 & \dots 101001100 \\ 0 & 0 & 2^3 & \dots 000001100 \\ 0 & 0 & 0 & 2^4 \end{pmatrix}$$

Manipulation de réseaux

Réduction de Hermite

$$\begin{pmatrix} 1 & 7 & 2 & 5 \\ 0 & 2^3 & 0 & 12 \\ 0 & 0 & 2^3 & 12 \\ 0 & 0 & 0 & 2^4 \end{pmatrix}$$

Manipulation de réseaux

Réduction de Hermite

$$\begin{pmatrix} 1 & 7 & 2 & 5 \\ 0 & 2^3 & 0 & 12 \\ 0 & 0 & 2^3 & 12 \\ 0 & 0 & 0 & 2^4 \end{pmatrix}$$

Corollaire

Les réseaux sont représentables de manière exacte

Manipulation de réseaux

Réduction de Hermite

$$\begin{pmatrix} 1 & 7 & 2 & 5 \\ 0 & 2^3 & 0 & 12 \\ 0 & 0 & 2^3 & 12 \\ 0 & 0 & 0 & 2^4 \end{pmatrix}$$

Corollaire

Les réseaux sont représentables de manière exacte

Mais aussi...

Manipulation de réseaux

Réduction de Hermite

$$\begin{pmatrix} 1 & 7 & 2 & 5 \\ 0 & 2^3 & 0 & 12 \\ 0 & 0 & 2^3 & 12 \\ 0 & 0 & 0 & 2^4 \end{pmatrix}$$

Corollaire

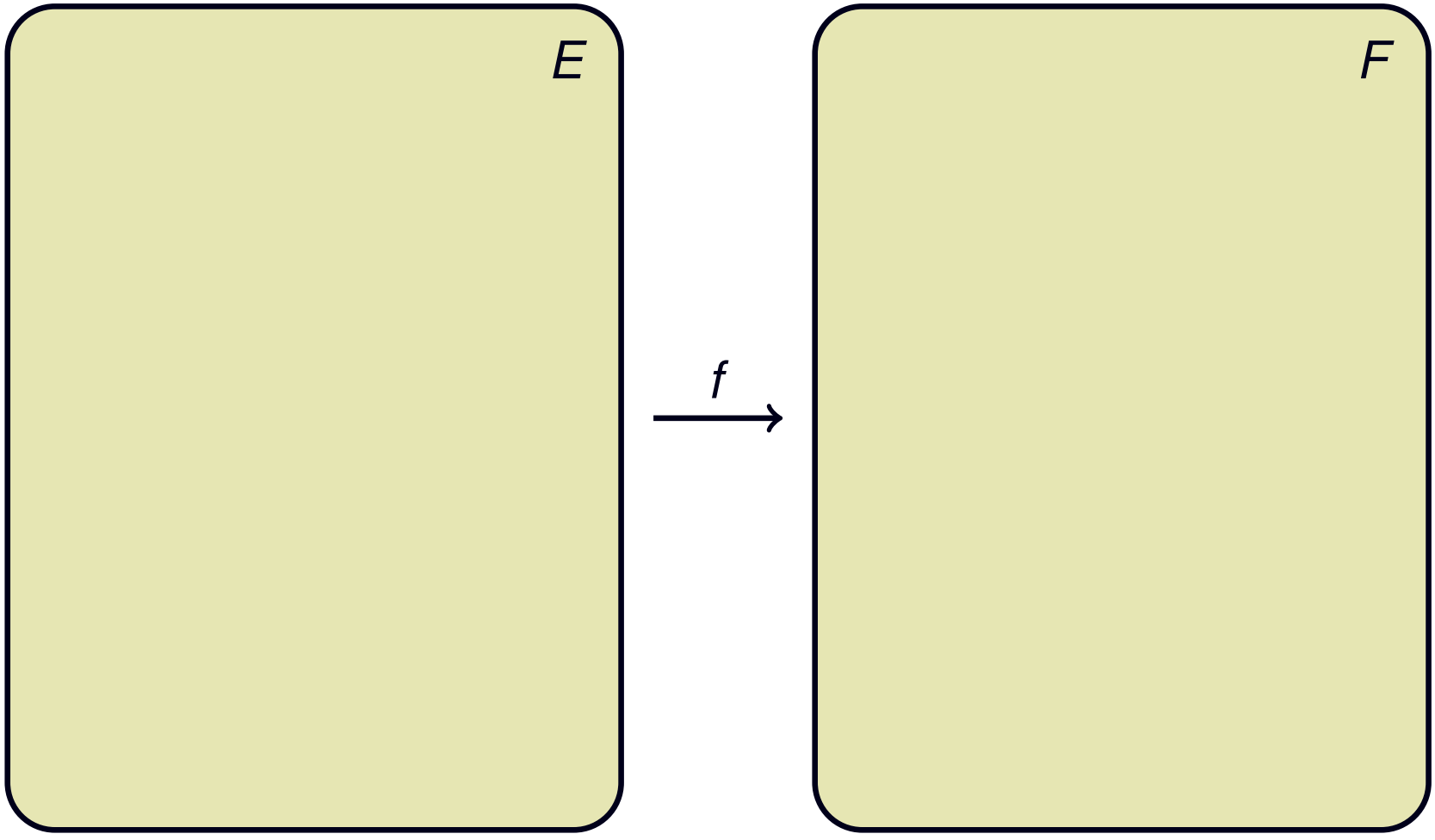
Les réseaux sont représentables de manière exacte

Mais aussi...

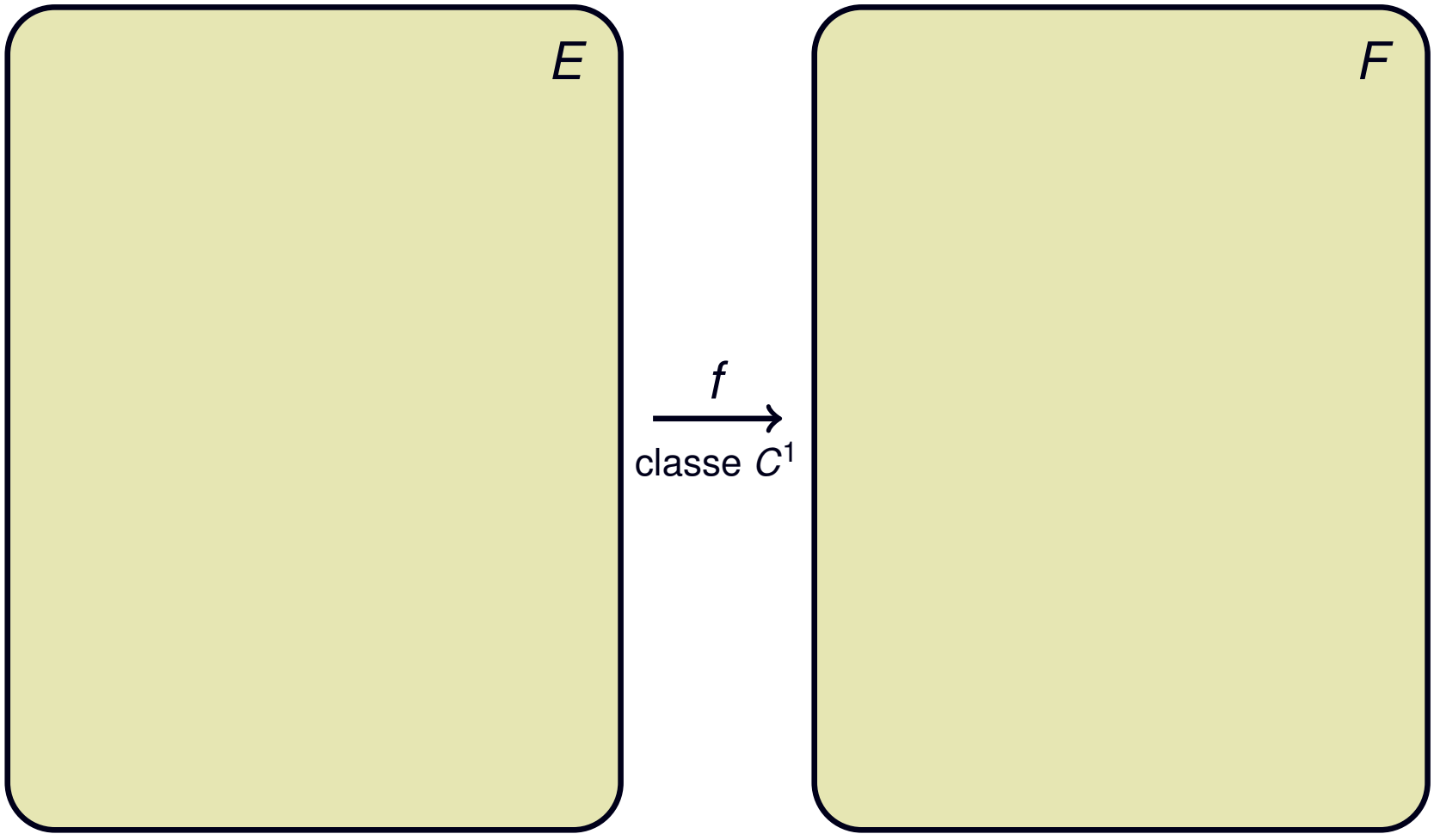
Les opérations sur les réseaux
(somme, intersection, image directe, image inverse)
sont aisément implémentables

Le lemme de précision

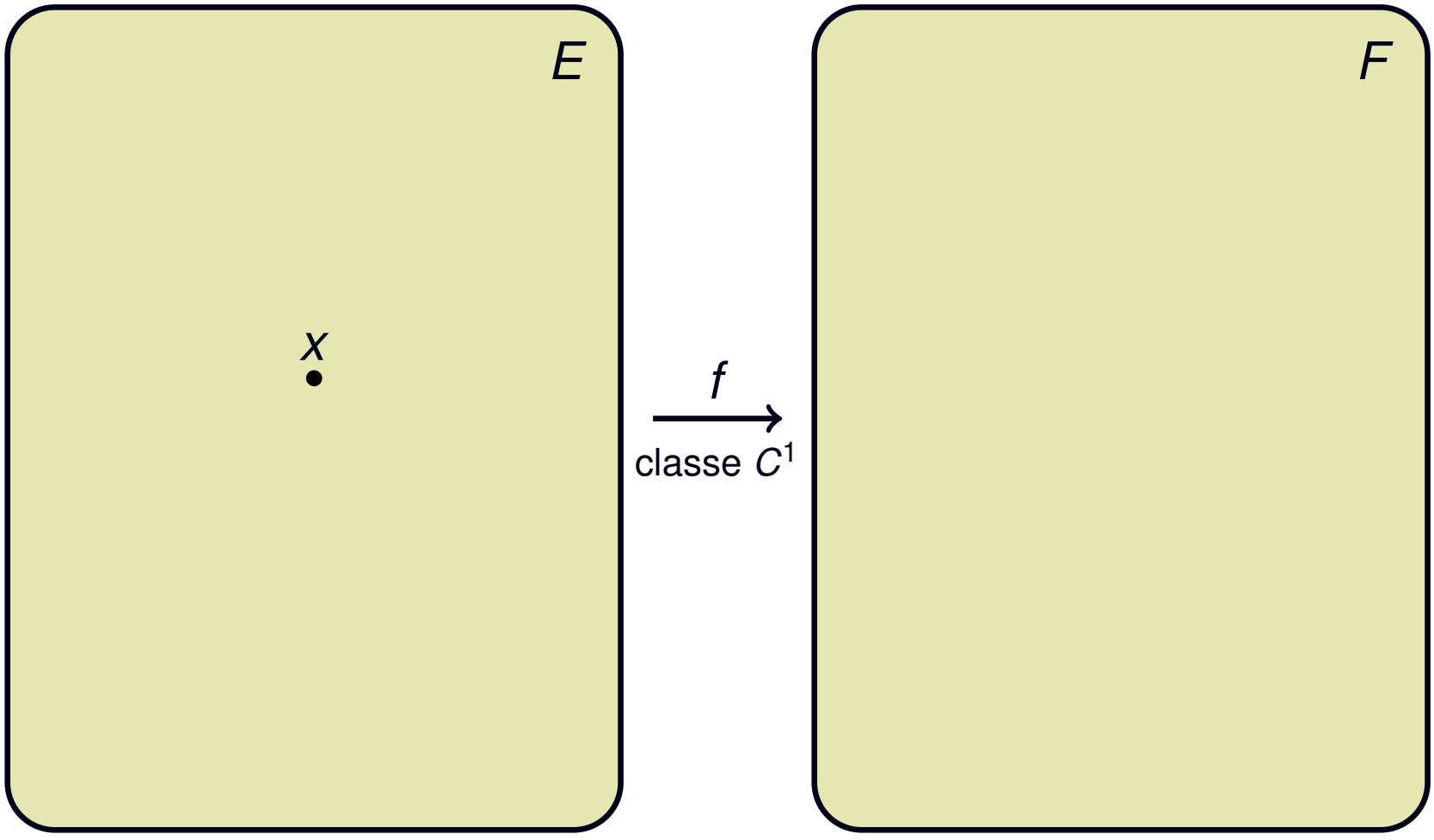
Le lemme de précision



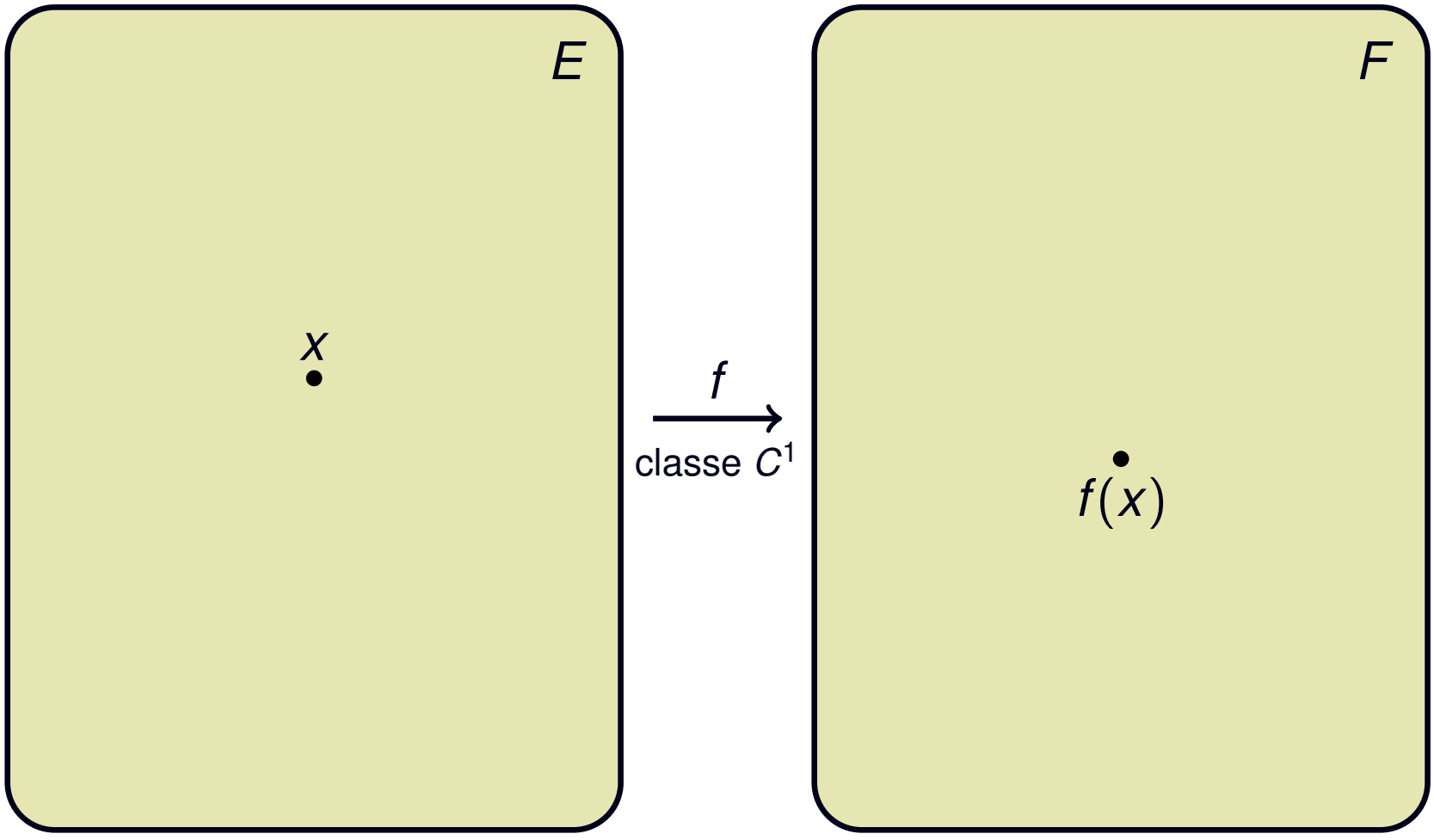
Le lemme de précision



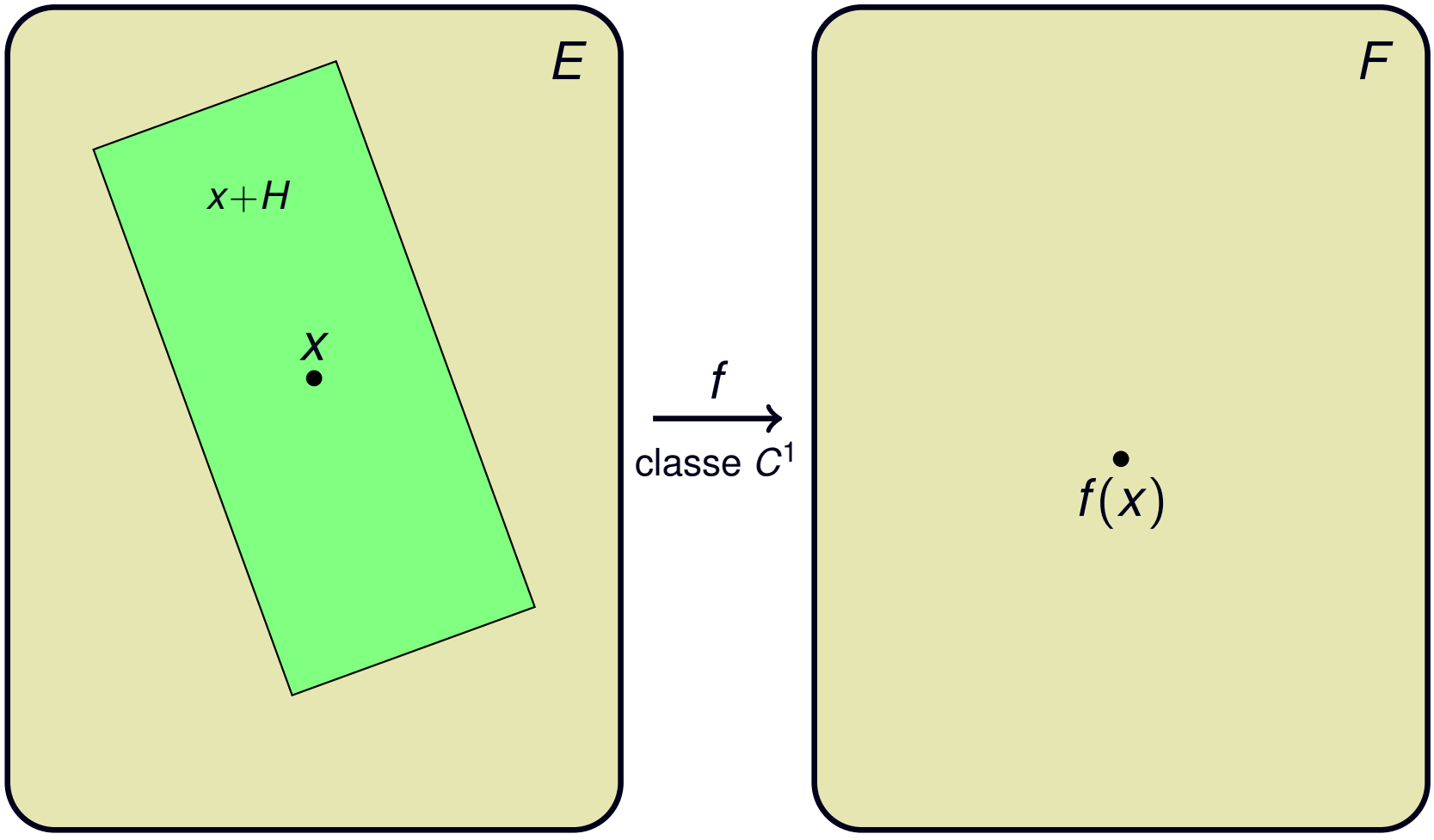
Le lemme de précision



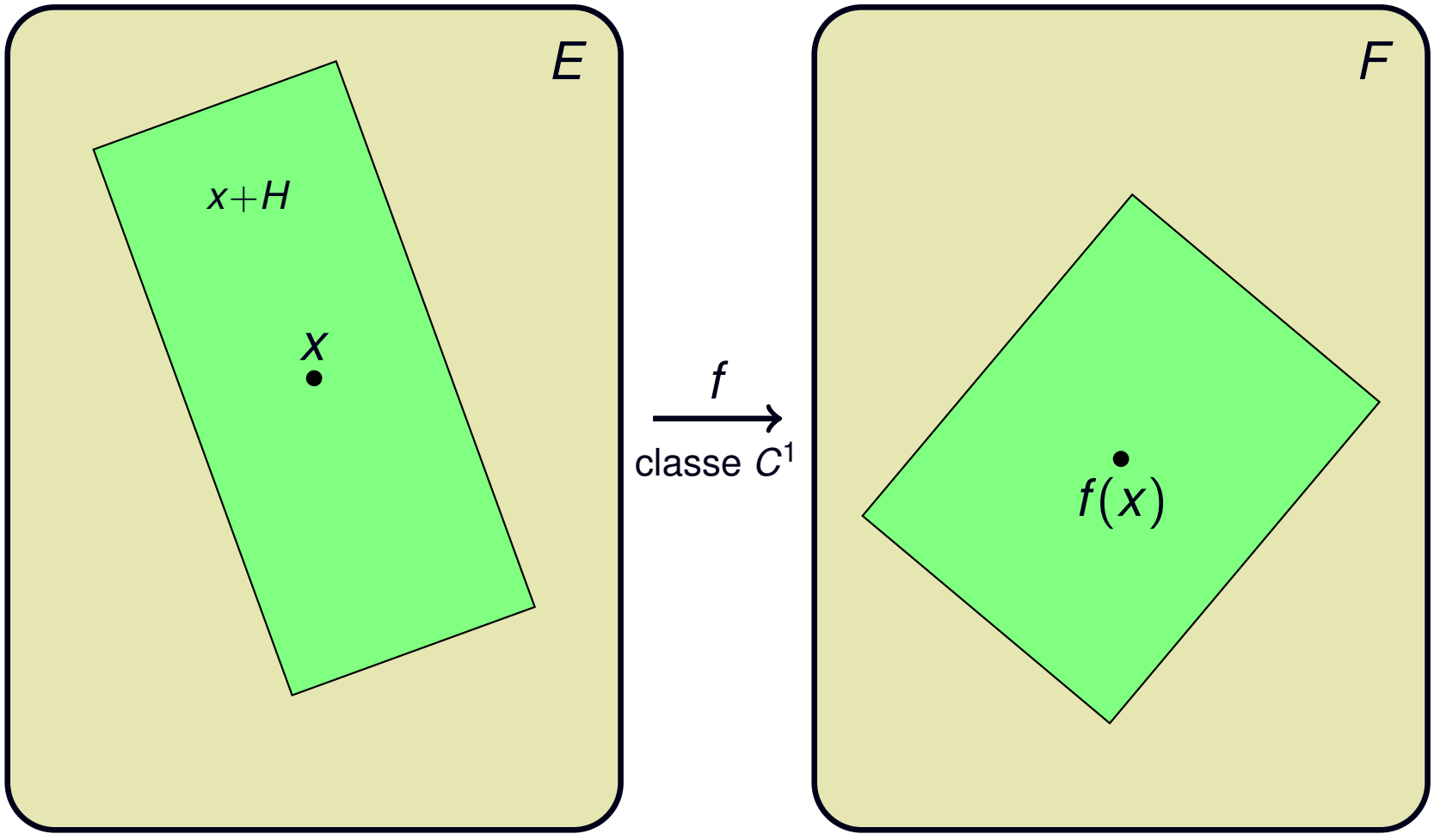
Le lemme de précision



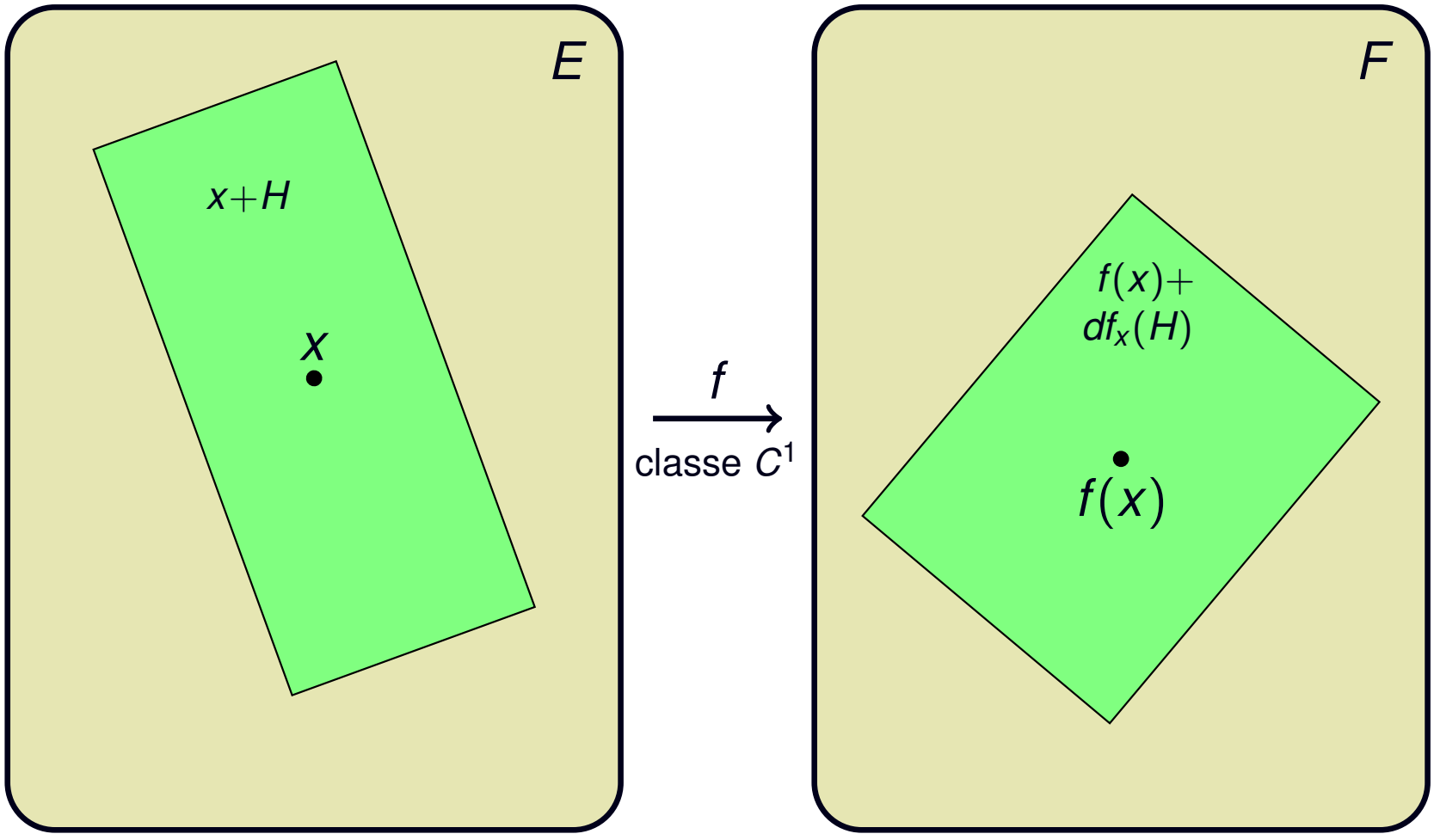
Le lemme de précision



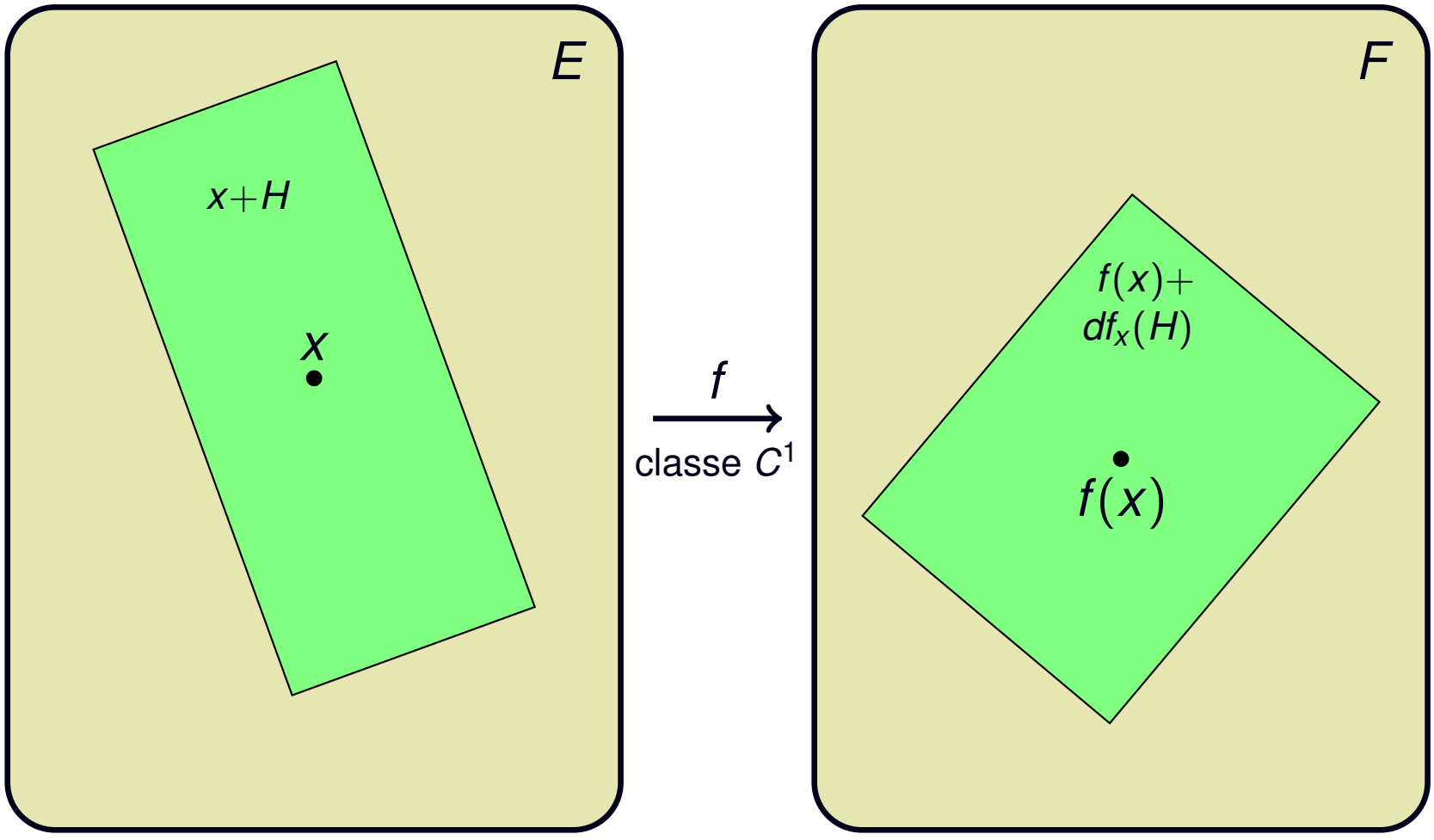
Le lemme de précision



Le lemme de précision

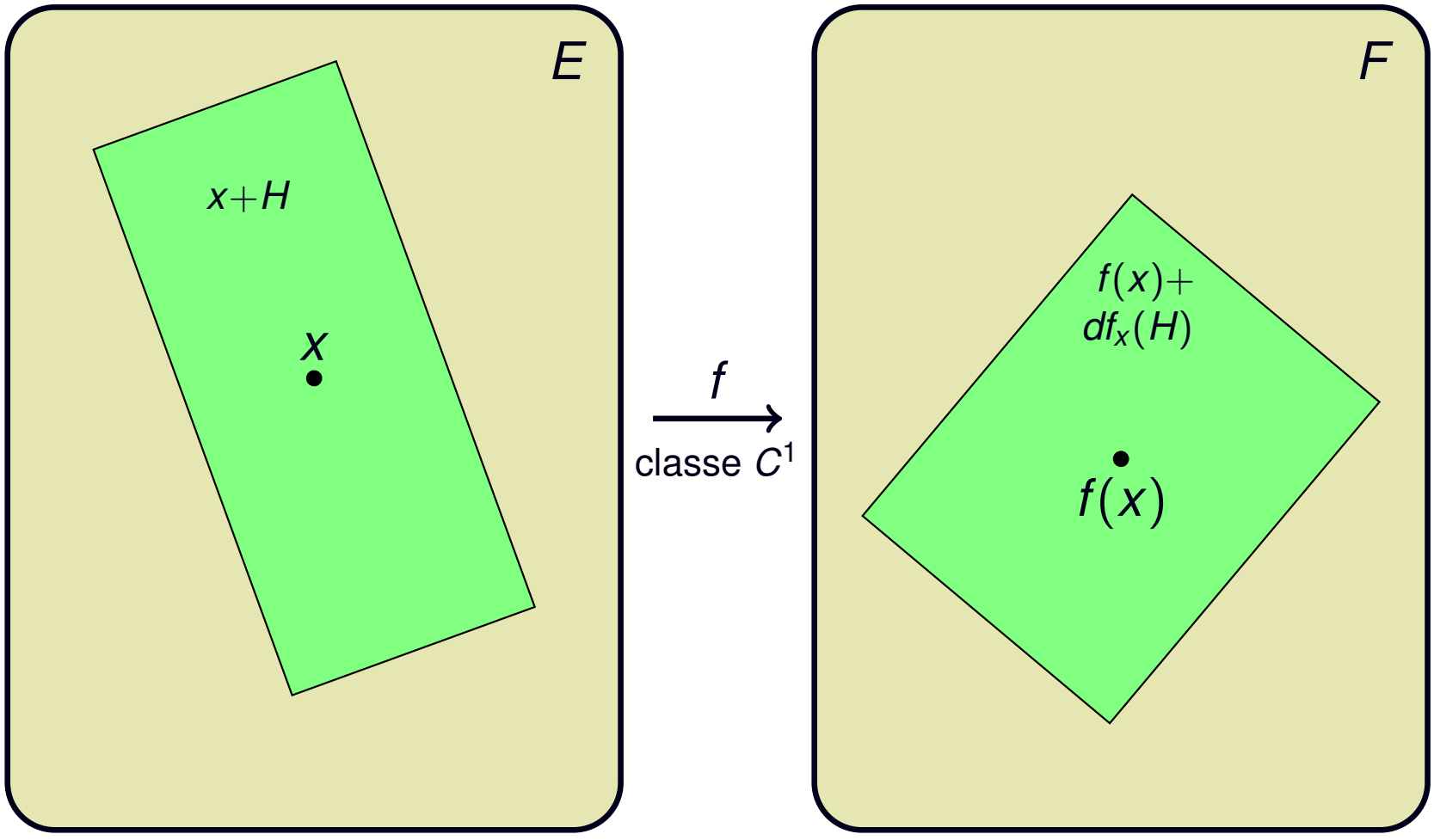


Le lemme de précision



$$f(x+H) = f(x) + df_x(H)$$

Le lemme de précision



$$f(x+H) = f(x) + df_x(H)$$

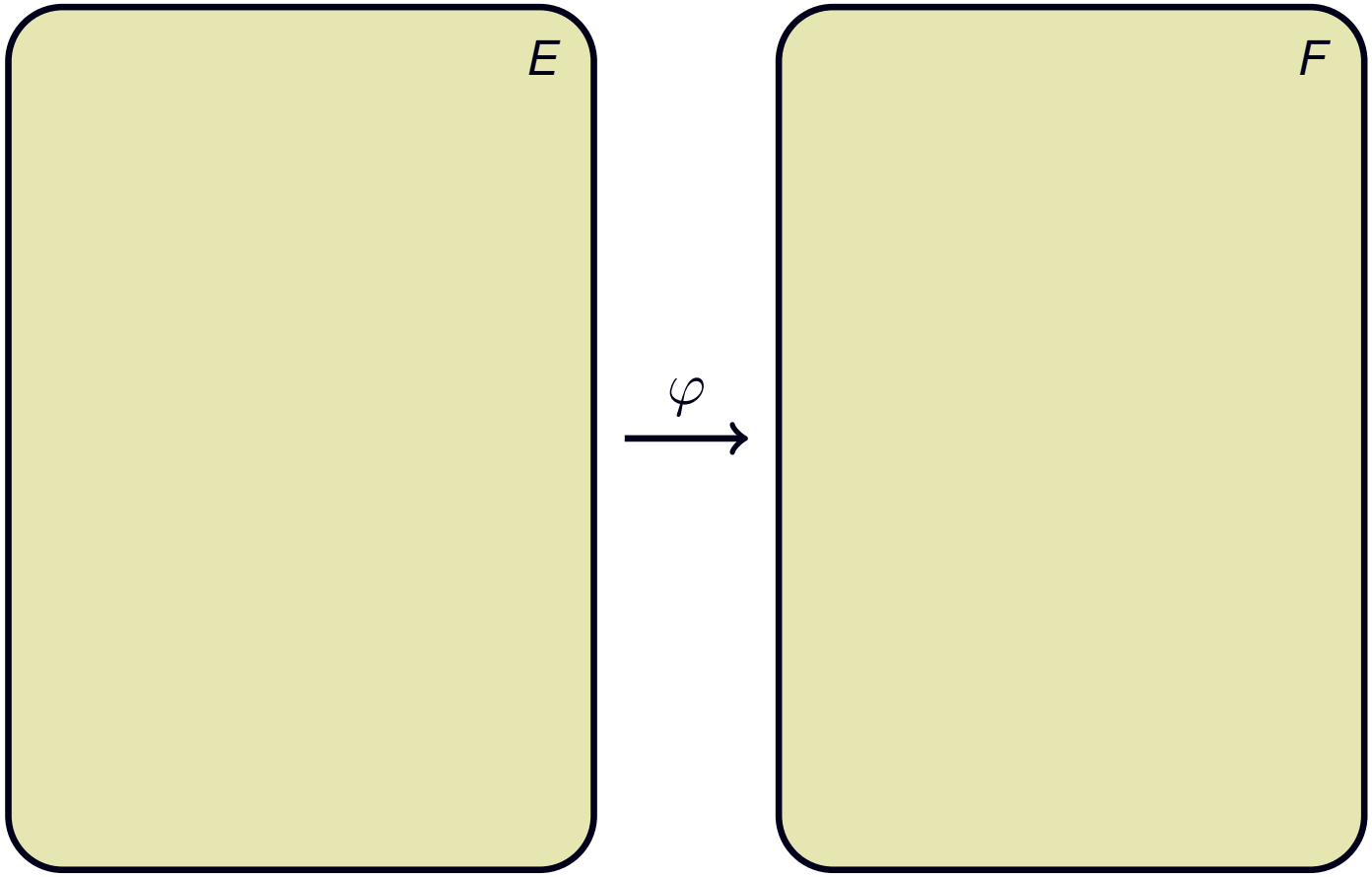
Hypothèses : df_x surjective, H suffisamment « bien »

Précision optimale

Contexte de l’arithmétique zélée

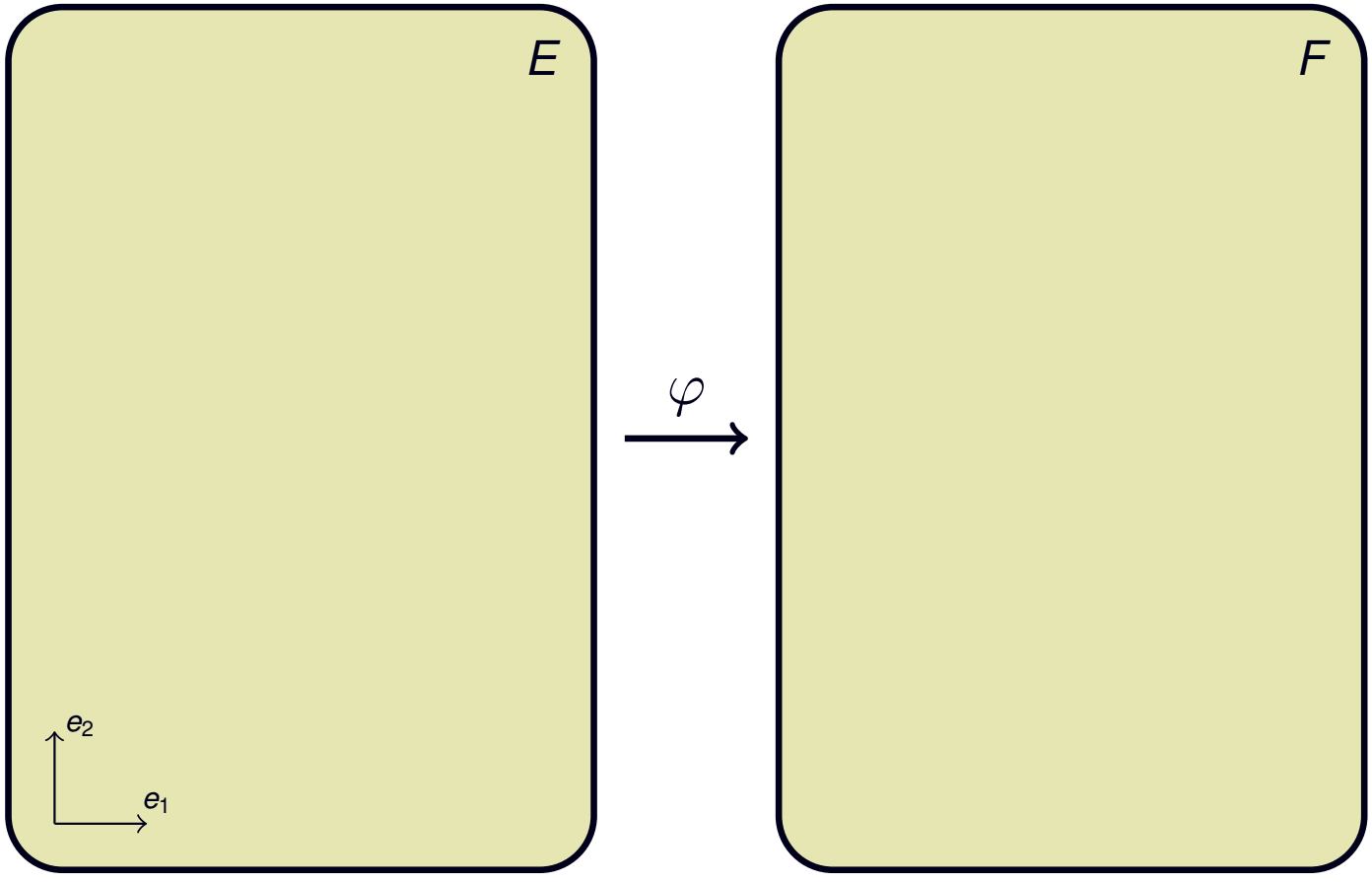
Précision optimale

Contexte de l'arithmétique zélée



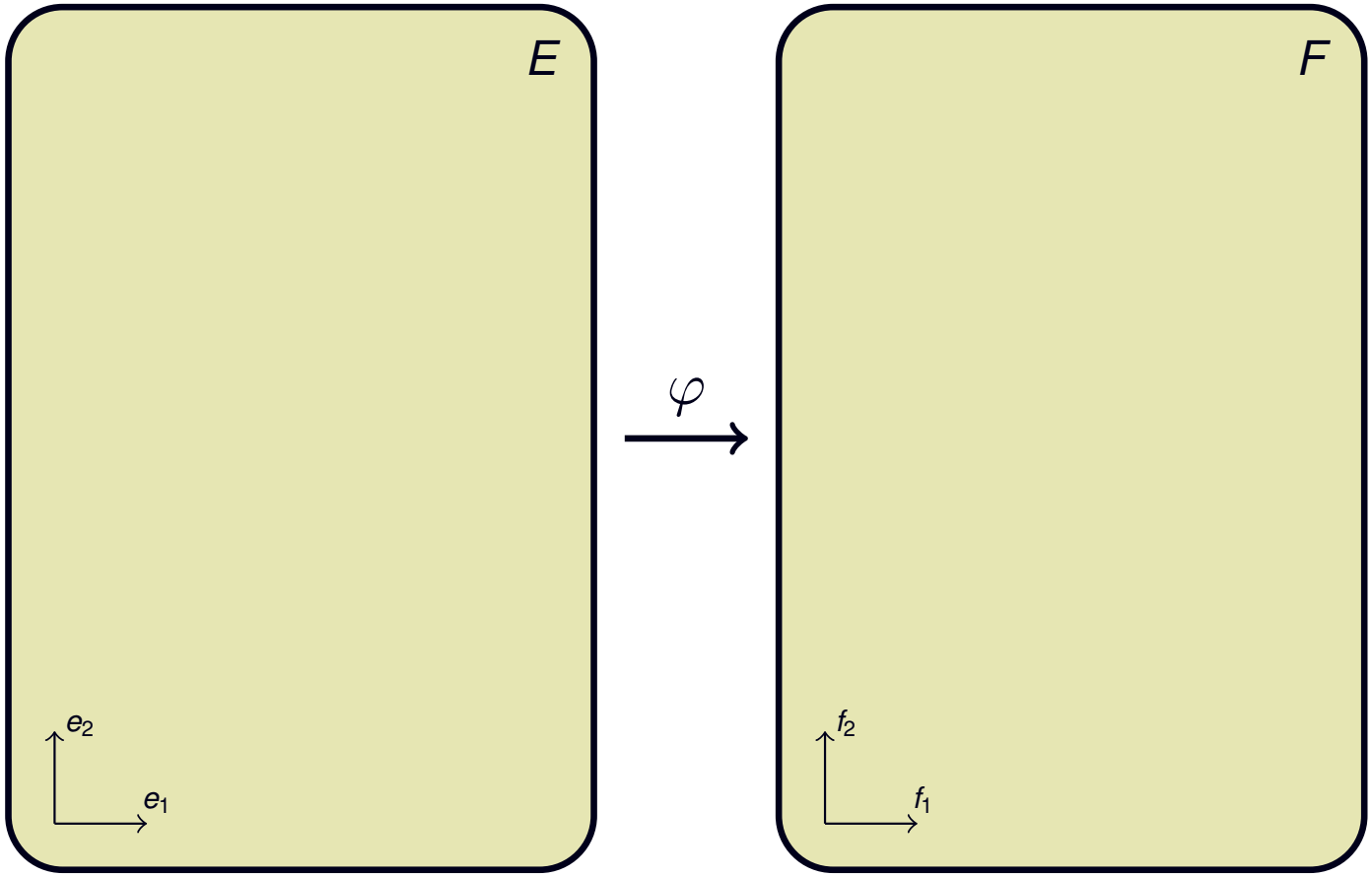
Précision optimale

Contexte de l'arithmétique zélée



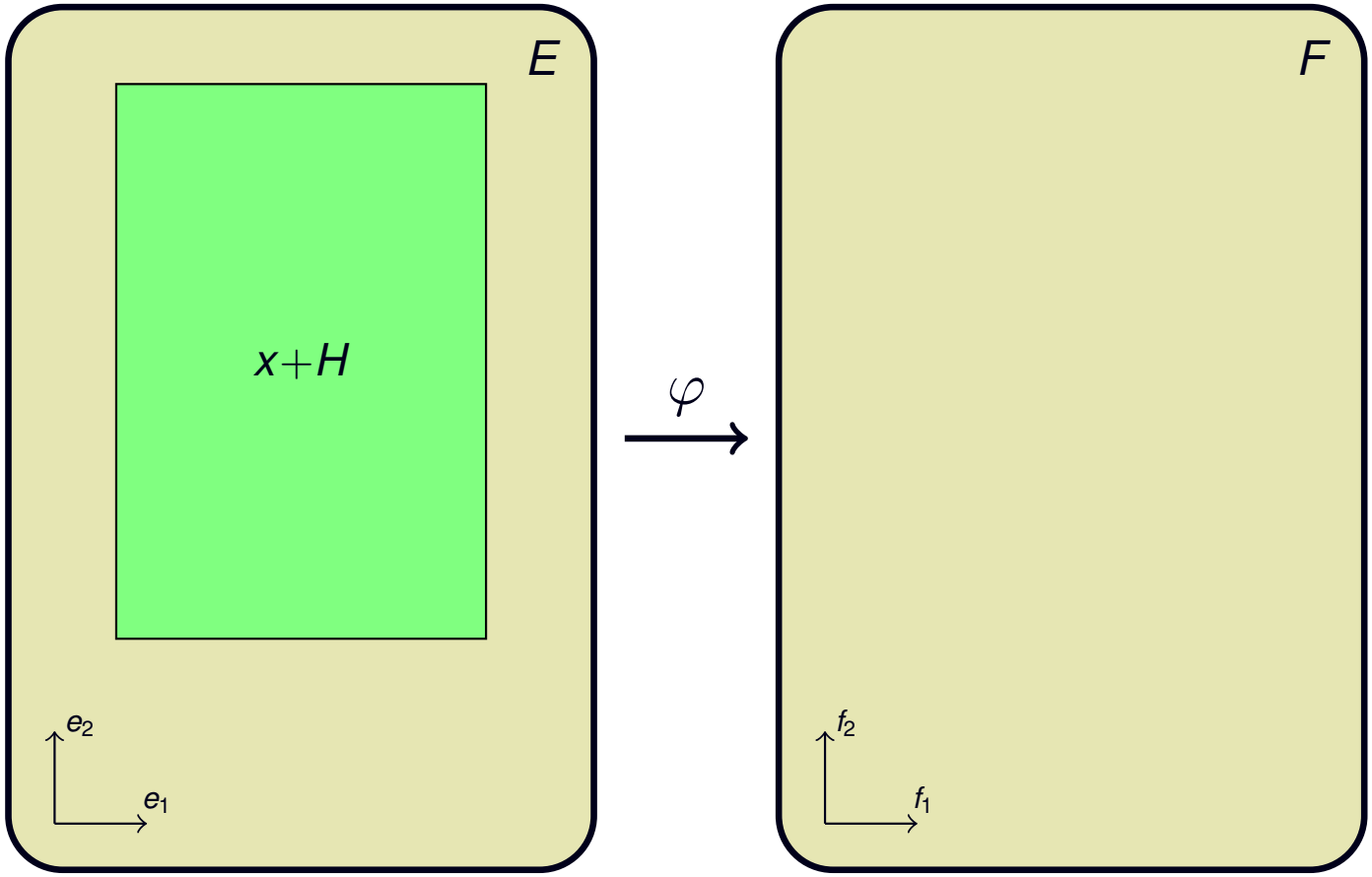
Précision optimale

Contexte de l'arithmétique zélée



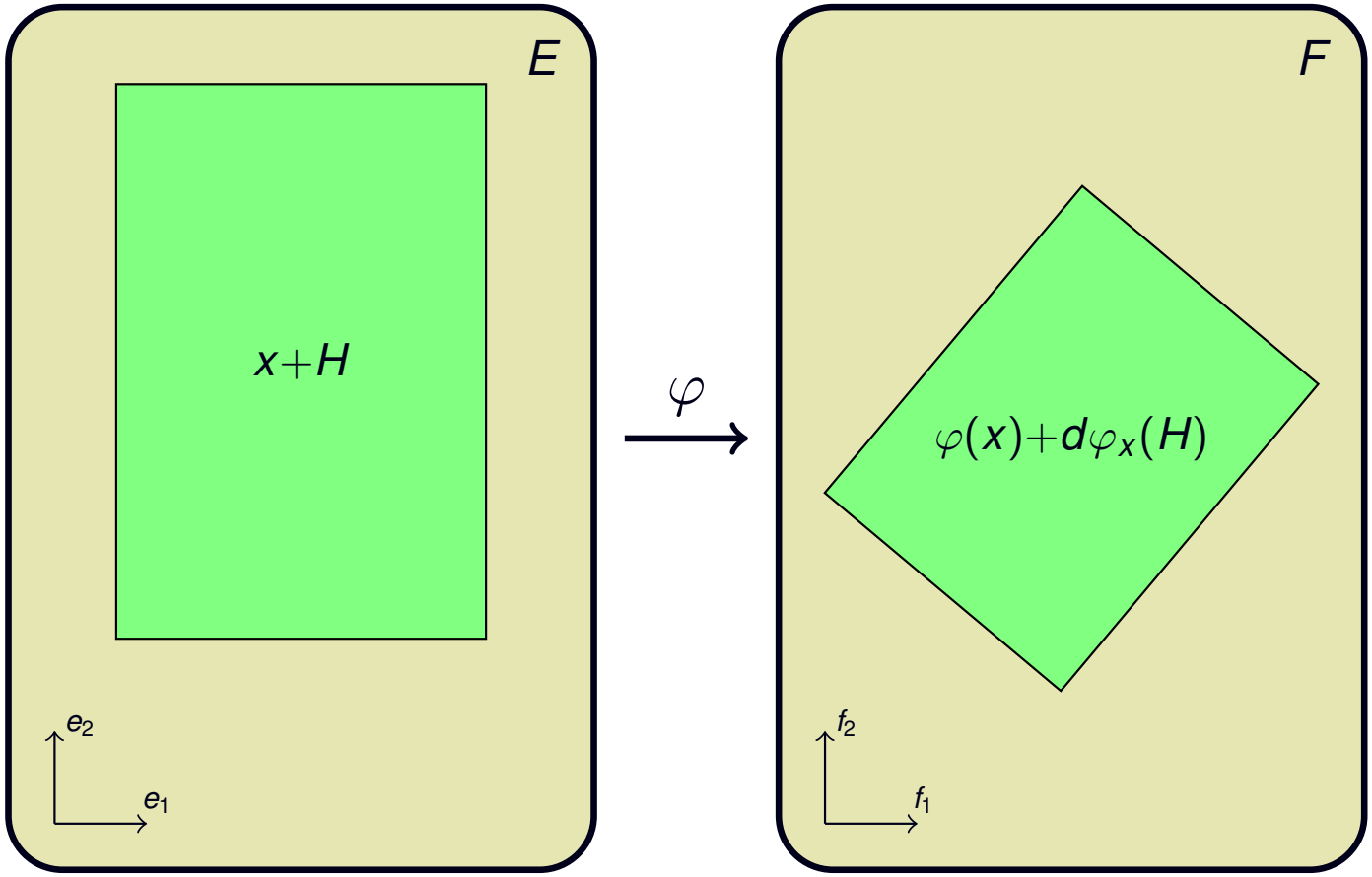
Précision optimale

Contexte de l'arithmétique zélée



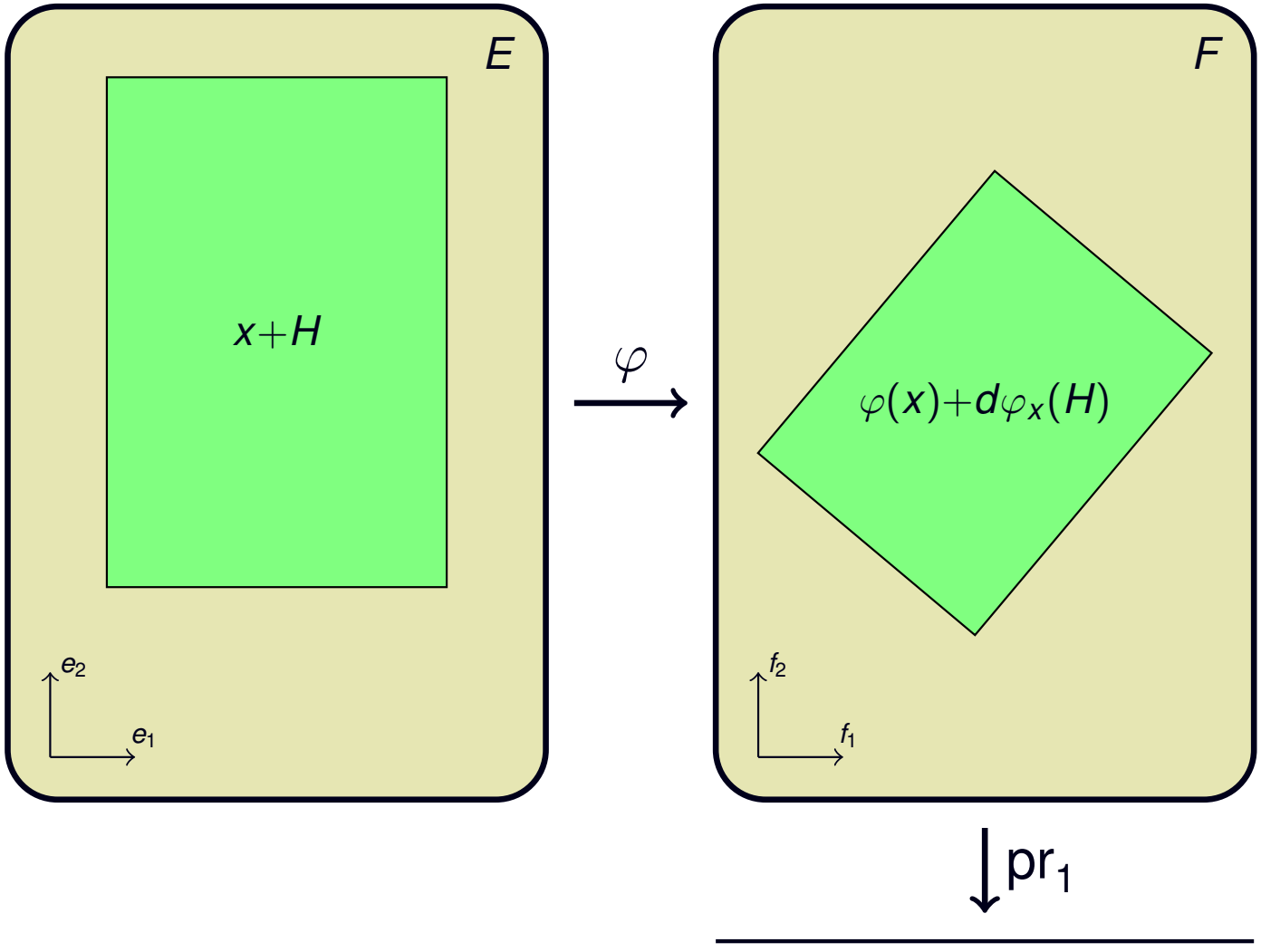
Précision optimale

Contexte de l'arithmétique zélée



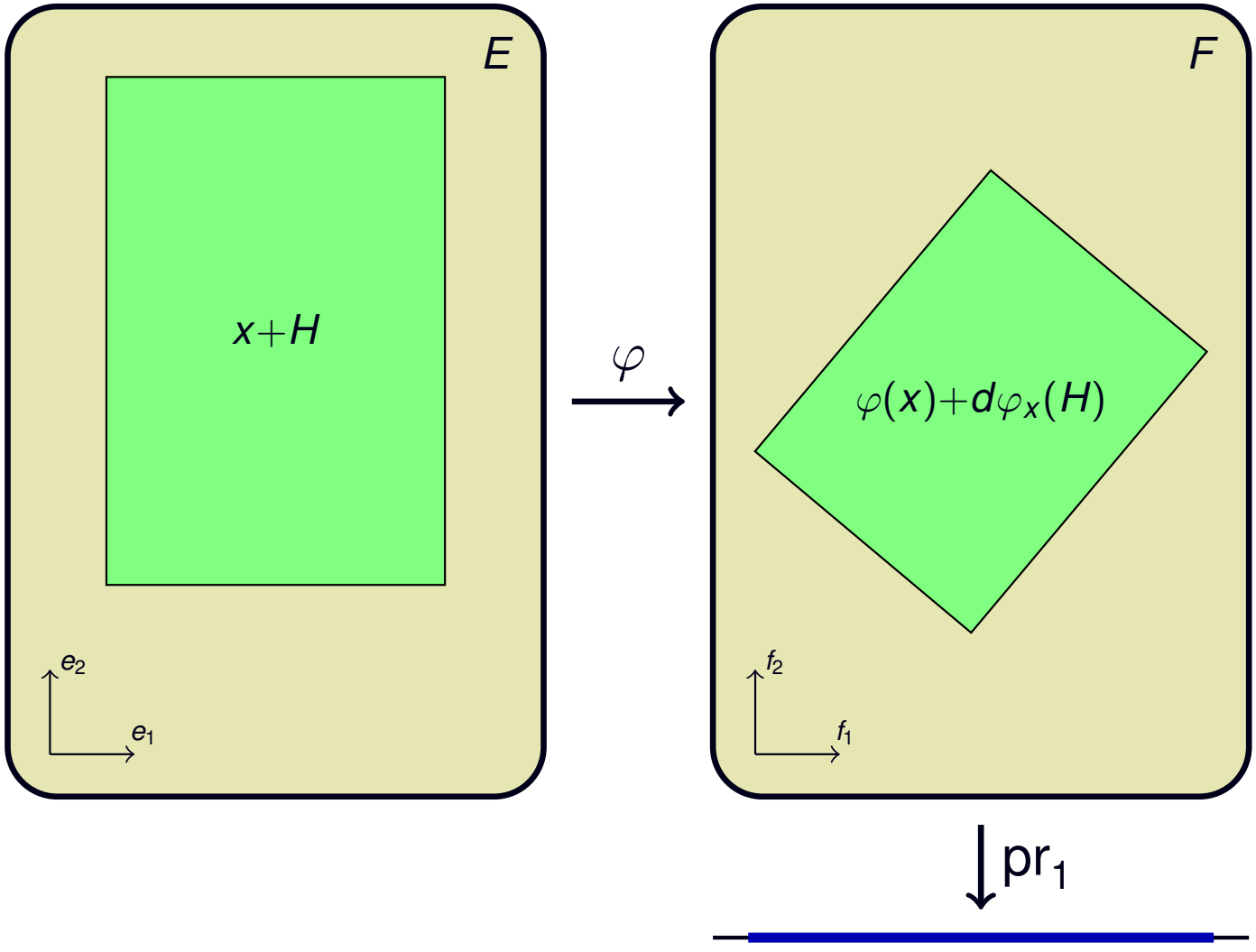
Précision optimale

Contexte de l'arithmétique zélée



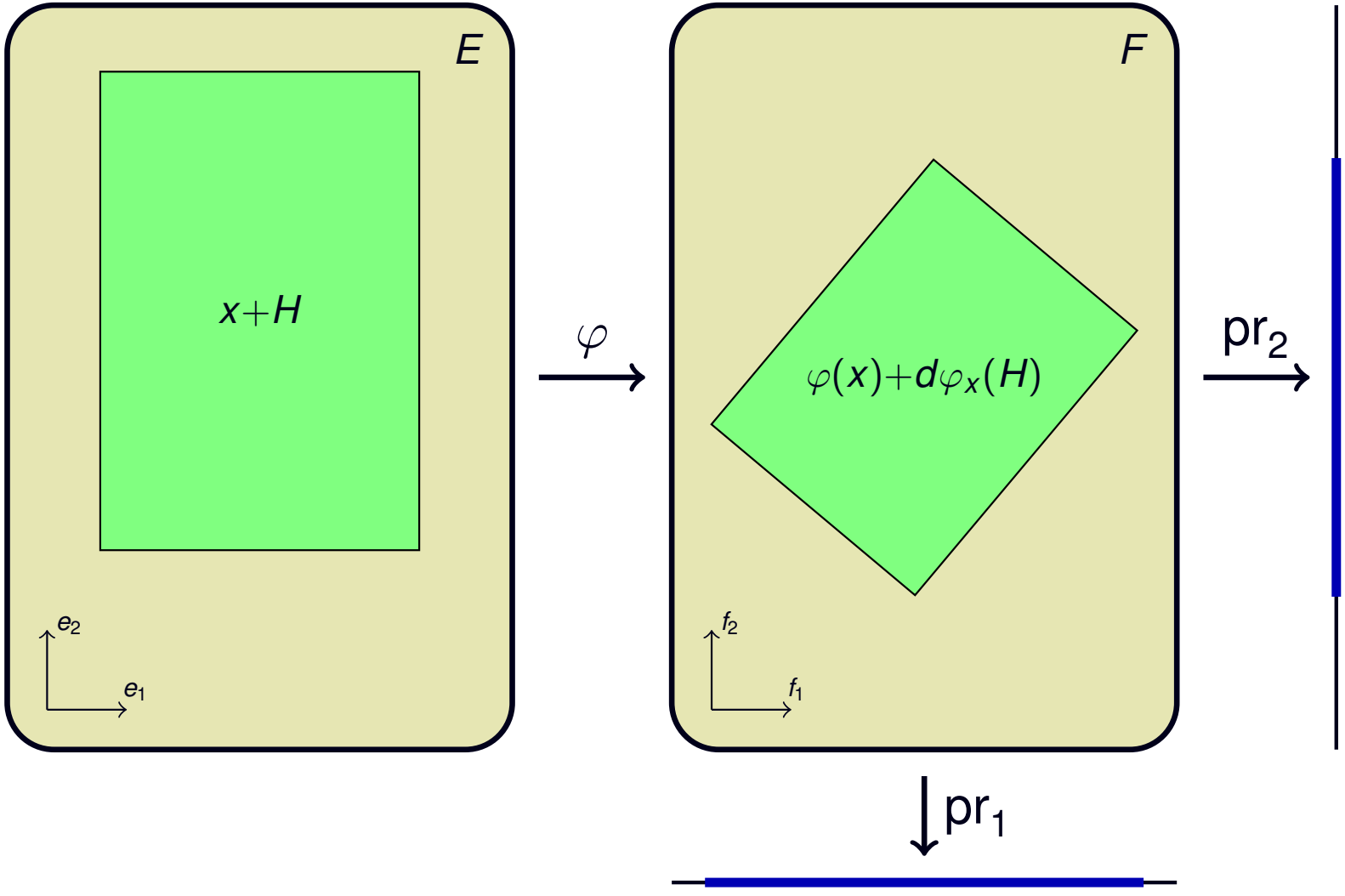
Précision optimale

Contexte de l'arithmétique zélée



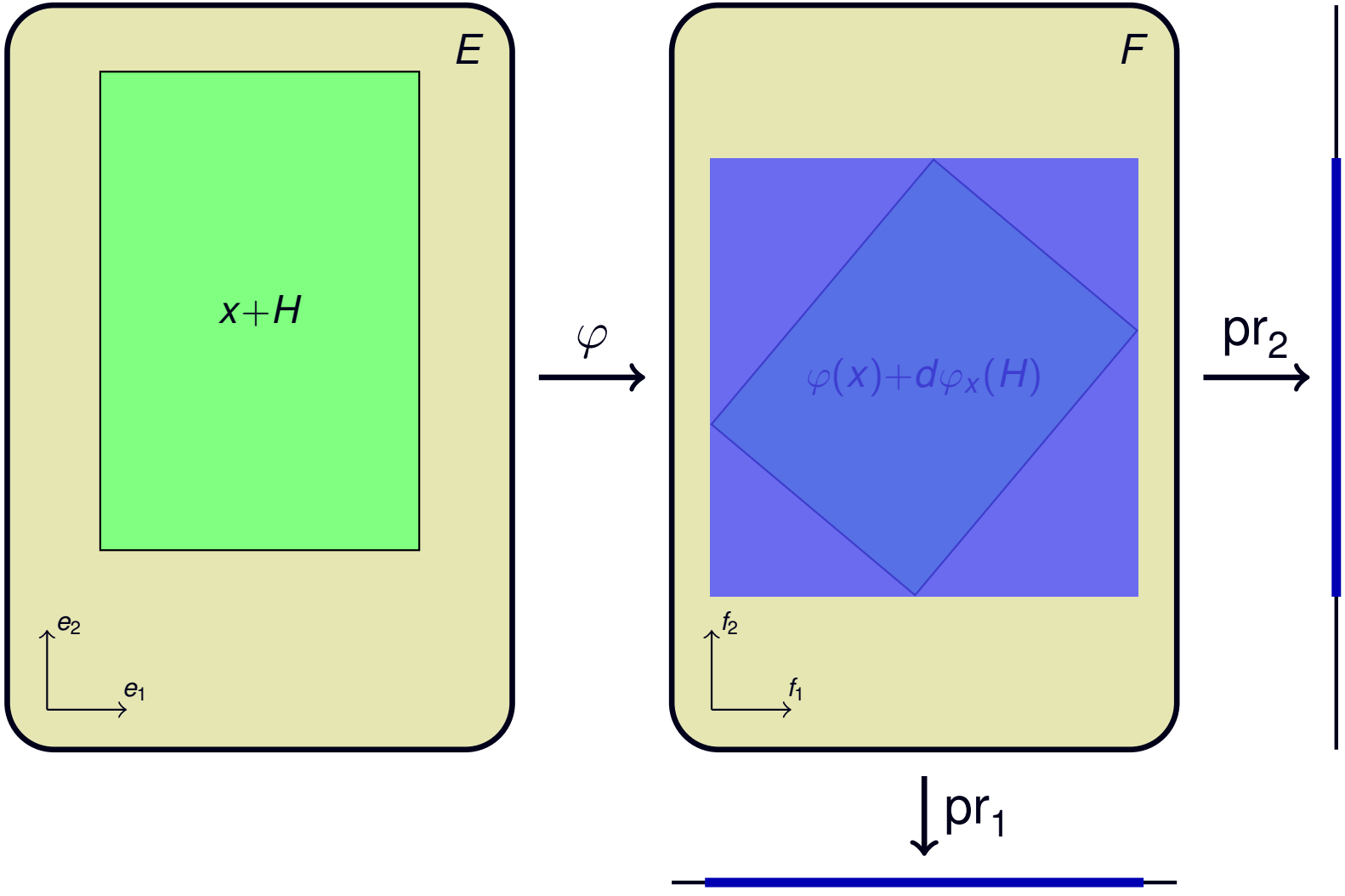
Précision optimale

Contexte de l'arithmétique zélée



Précision optimale

Contexte de l'arithmétique zélée



Précision optimale

Contexte de l’arithmétique zélée

Précision optimale

Contexte de l'arithmétique zélée

$$\begin{pmatrix} p^{N_1} & & \\ & \ddots & \\ & & p^{N_n} \end{pmatrix}$$

Précision optimale

Contexte de l'arithmétique zélée

$$\begin{pmatrix} p^{N_1} & & \\ & \ddots & \\ & & p^{N_n} \end{pmatrix} \cdot J(\varphi)_x$$

Précision optimale

Contexte de l'arithmétique zélée

$$\begin{pmatrix} p^{N_1} & & \\ & \ddots & \\ & & p^{N_n} \end{pmatrix} \cdot J(\varphi)_x$$

$$= \begin{pmatrix} & & \\ & & \\ & & \end{pmatrix}$$

Précision optimale

Contexte de l'arithmétique zélée

$$\begin{pmatrix} p^{N_1} & & \\ & \ddots & \\ & & p^{N_n} \end{pmatrix} \cdot J(\varphi)_x$$

$$= \begin{pmatrix} L_1 \\ \hdots \\ \vdots \\ \hdots \\ L_n \end{pmatrix}$$

Précision optimale

Contexte de l'arithmétique zélée

$$\begin{pmatrix} p^{N_1} & & \\ & \ddots & \\ & & p^{N_n} \end{pmatrix} \cdot J(\varphi)_x$$

$$= \left(\begin{array}{c:c:c:c} C_1 & C_2 & \cdots & C_m \end{array} \right)$$

Précision optimale
Contexte de l'arithmétique zélée

$$\begin{pmatrix} p^{N_1} & & \\ & \ddots & \\ & & p^{N_n} \end{pmatrix} \cdot J(\varphi)_x$$

$$= \left(\begin{array}{c:c:c:c} C_1 & C_2 & \cdots & C_m \end{array} \right)$$

Précision optimale sur la j-ième composante de $\varphi(x)$:

$$O\left(p^{\mathrm{val}(C_j)}\right)$$

Exemple jouet

Exemple jouet

$$\begin{array}{rccc} \varphi : & \mathbb{Q}_p[X]_{\leq 1} & \longrightarrow & \mathbb{Q}_p^2 \\ & P(X) & \mapsto & \big(P(0), P(p)\big) \end{array}$$

Exemple jouet

$$\begin{array}{rccc} \varphi : & \mathbb{Q}_p[X]_{\leq 1} & \longrightarrow & \mathbb{Q}_p^2 \\ & P(X) & \mapsto & \big(P(0), P(p)\big) \\ & aX + b & \mapsto & \big(b, ap + b\big) \end{array}$$

Exemple jouet

$$\begin{array}{rccc} \varphi : & \mathbb{Q}_p[X]_{\leq 1} & \longrightarrow & \mathbb{Q}_p^2 \\ & P(X) & \mapsto & \big(P(0), P(p)\big) \\ & aX + b & \mapsto & \big(b, ap + b\big) \end{array}$$

Jacobienne

$$J(\varphi) = \begin{pmatrix} 0 & p \\ 1 & 1 \end{pmatrix}$$

Exemple jouet

$$\begin{array}{rccc} \varphi : & \mathbb{Q}_p[X]_{\leq 1} & \longrightarrow & \mathbb{Q}_p^2 \\ & P(X) & \mapsto & \big(P(0), P(p)\big) \\ & aX + b & \mapsto & \big(b, ap + b\big) \end{array}$$

Jacobienne

$$J(\varphi) = \begin{pmatrix} 0 & p \\ 1 & 1 \end{pmatrix}$$

Conséquence sur la précision

Exemple jouet

$$\begin{array}{rccc} \varphi : & \mathbb{Q}_p[X]_{\leq 1} & \longrightarrow & \mathbb{Q}_p^2 \\ & P(X) & \mapsto & \big(P(0), P(p)\big) \\ & aX + b & \mapsto & \big(b, ap + b\big) \end{array}$$

Jacobienne

$$J(\varphi) = \begin{pmatrix} 0 & p \\ 1 & 1 \end{pmatrix}$$

Conséquence sur la précision

Si a et b sont donnés à précision $O(p^N)$, alors :

Exemple jouet

$$\begin{array}{rccc} \varphi : & \mathbb{Q}_p[X]_{\leq 1} & \longrightarrow & \mathbb{Q}_p^2 \\ & P(X) & \mapsto & \big(P(0), P(p)\big) \\ & aX + b & \mapsto & \big(b, ap + b\big) \end{array}$$

Jacobienne

$$J(\varphi) = \begin{pmatrix} 0 & p \\ 1 & 1 \end{pmatrix}$$

Conséquence sur la précision

Si a et b sont donnés à précision $O(p^N)$, alors :

$$P(0) \quad \text{est connu à précision} \quad O(p^N)$$

Exemple jouet

$$\begin{array}{rccc} \varphi : & \mathbb{Q}_p[X]_{\leq 1} & \longrightarrow & \mathbb{Q}_p^2 \\ & P(X) & \mapsto & \big(P(0), P(p)\big) \\ & aX + b & \mapsto & \big(b, ap + b\big) \end{array}$$

Jacobienne

$$J(\varphi) = \begin{pmatrix} 0 & p \\ 1 & 1 \end{pmatrix}$$

Conséquence sur la précision

Si a et b sont donnés à précision $O(p^N)$, alors :

$$\begin{array}{lll} P(0) & \text{est connu à précision} & O(p^N) \\ P(p) & \text{\_\_\_\_\_} & O(p^N) \end{array}$$

Exemple jouet

$$\begin{array}{rccc} \varphi : & \mathbb{Q}_p[X]_{\leq 1} & \longrightarrow & \mathbb{Q}_p^2 \\ & P(X) & \mapsto & \big(P(0), P(p)\big) \\ & aX + b & \mapsto & \big(b, ap + b\big) \end{array}$$

Jacobienne

$$J(\varphi) = \begin{pmatrix} 0 & p \\ 1 & 1 \end{pmatrix}$$

Conséquence sur la précision

Si a et b sont donnés à précision $O(p^N)$, alors :

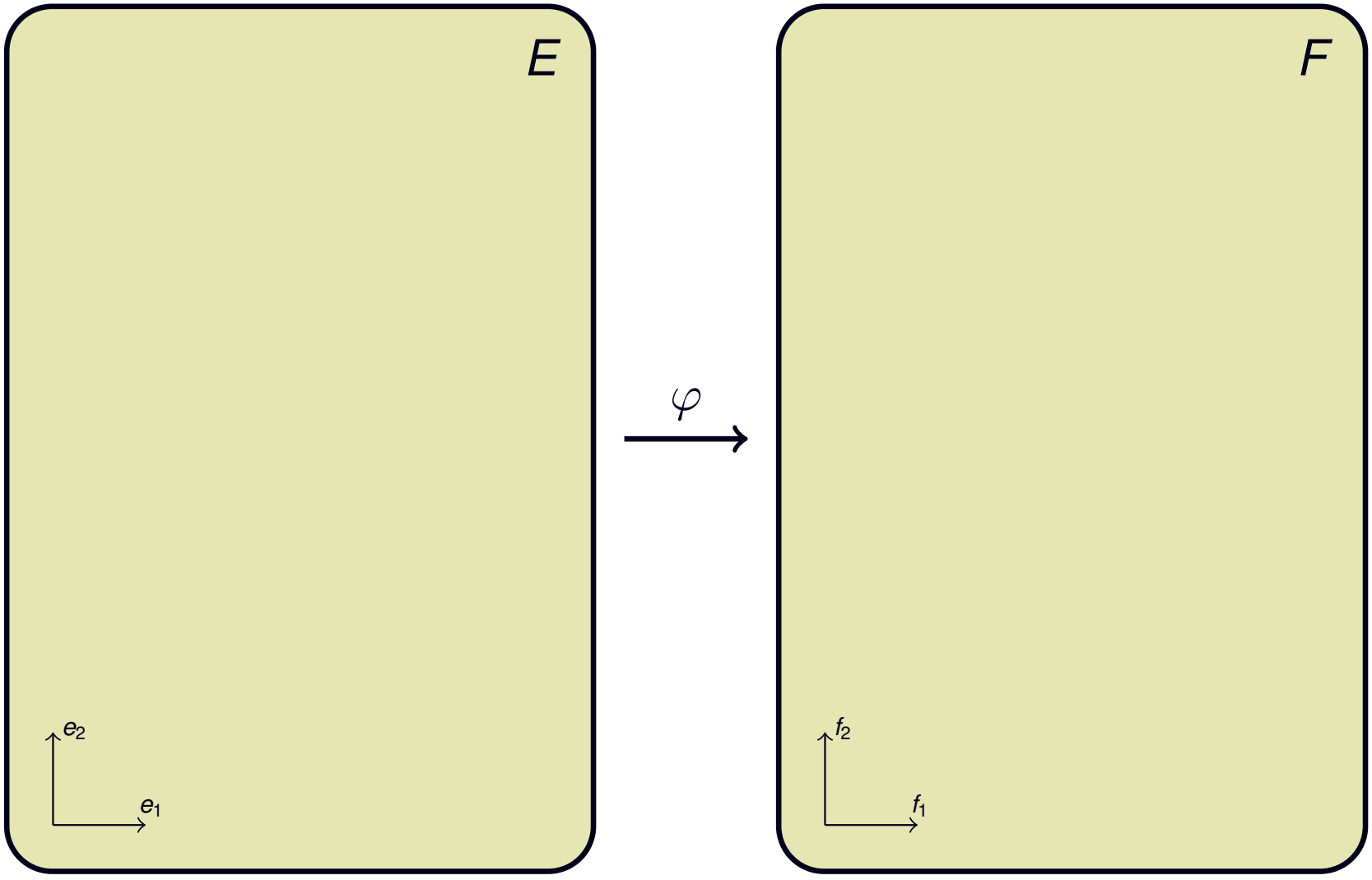
$$\begin{array}{lrll} & P(0) & \text{est connu à précision} & O(p^N) \\ & P(p) & \text{\_\_\_\_\_} & O(p^N) \\ \textbf{mais} & P(p)-P(0) & \text{\_\_\_\_\_} & O(p^{N+1}) \end{array}$$

Précision optimale

Contexte de l’arithmétique paresseuse

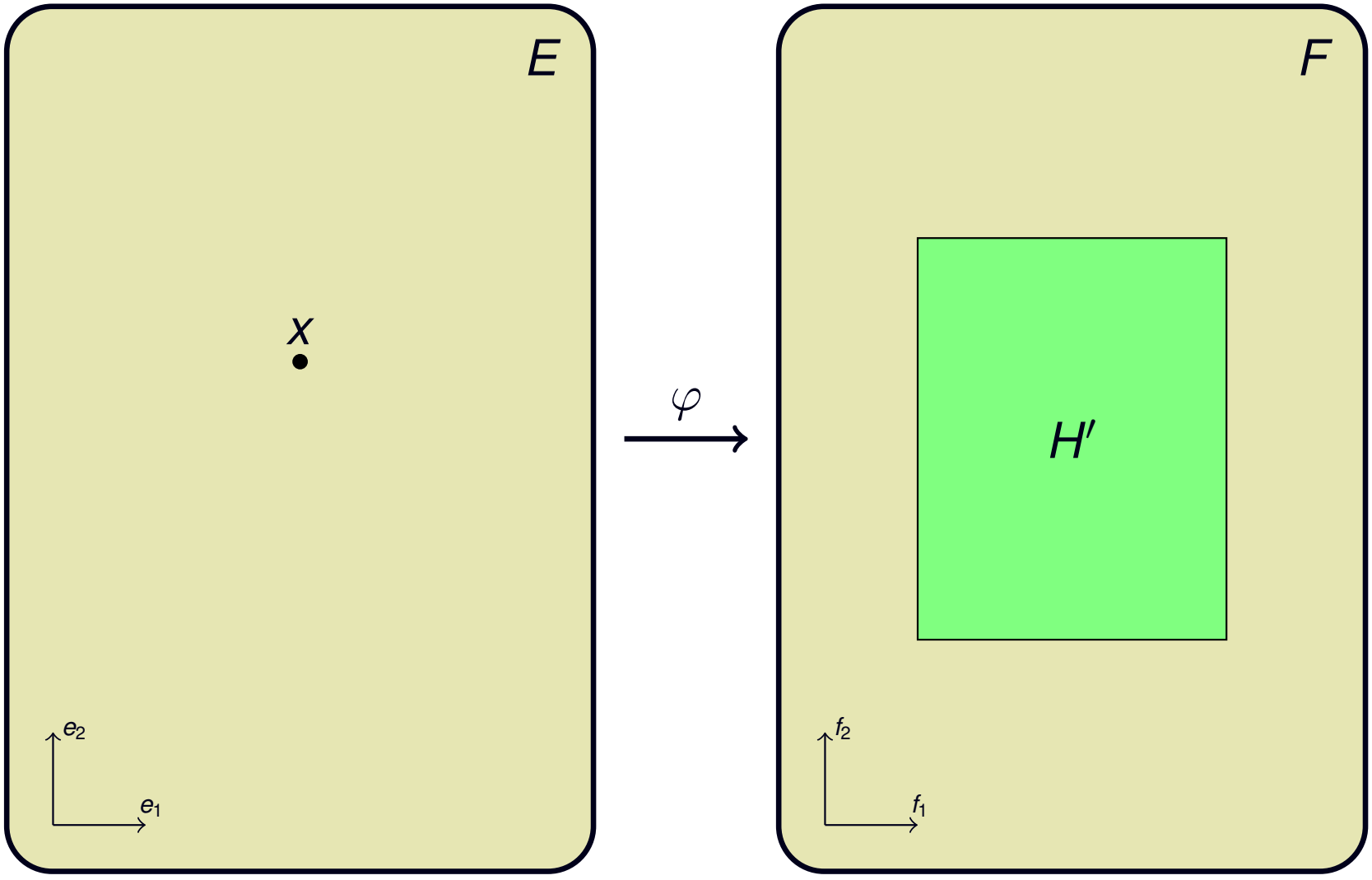
Précision optimale

Contexte de l'arithmétique paresseuse



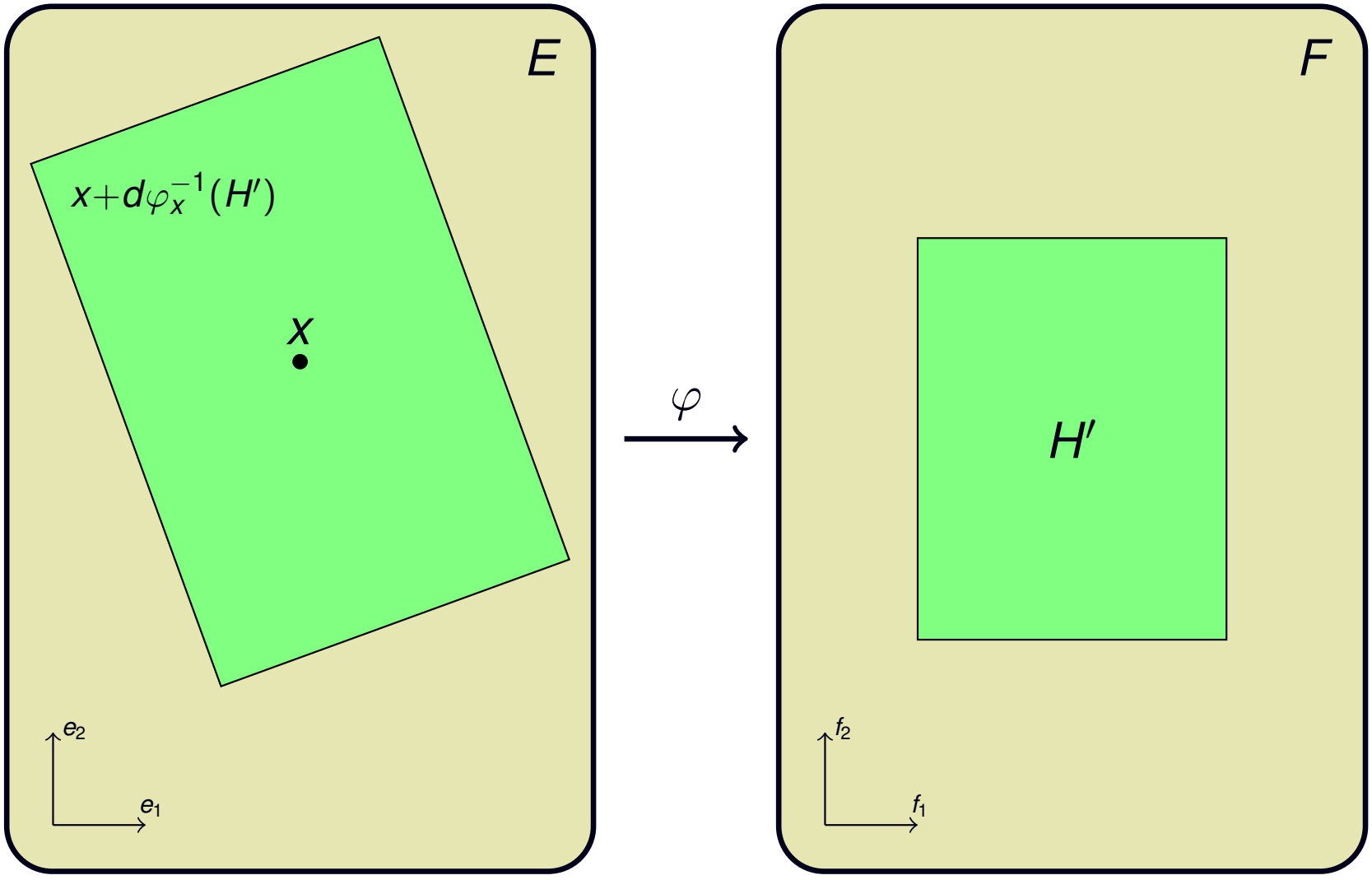
Précision optimale

Contexte de l'arithmétique paresseuse



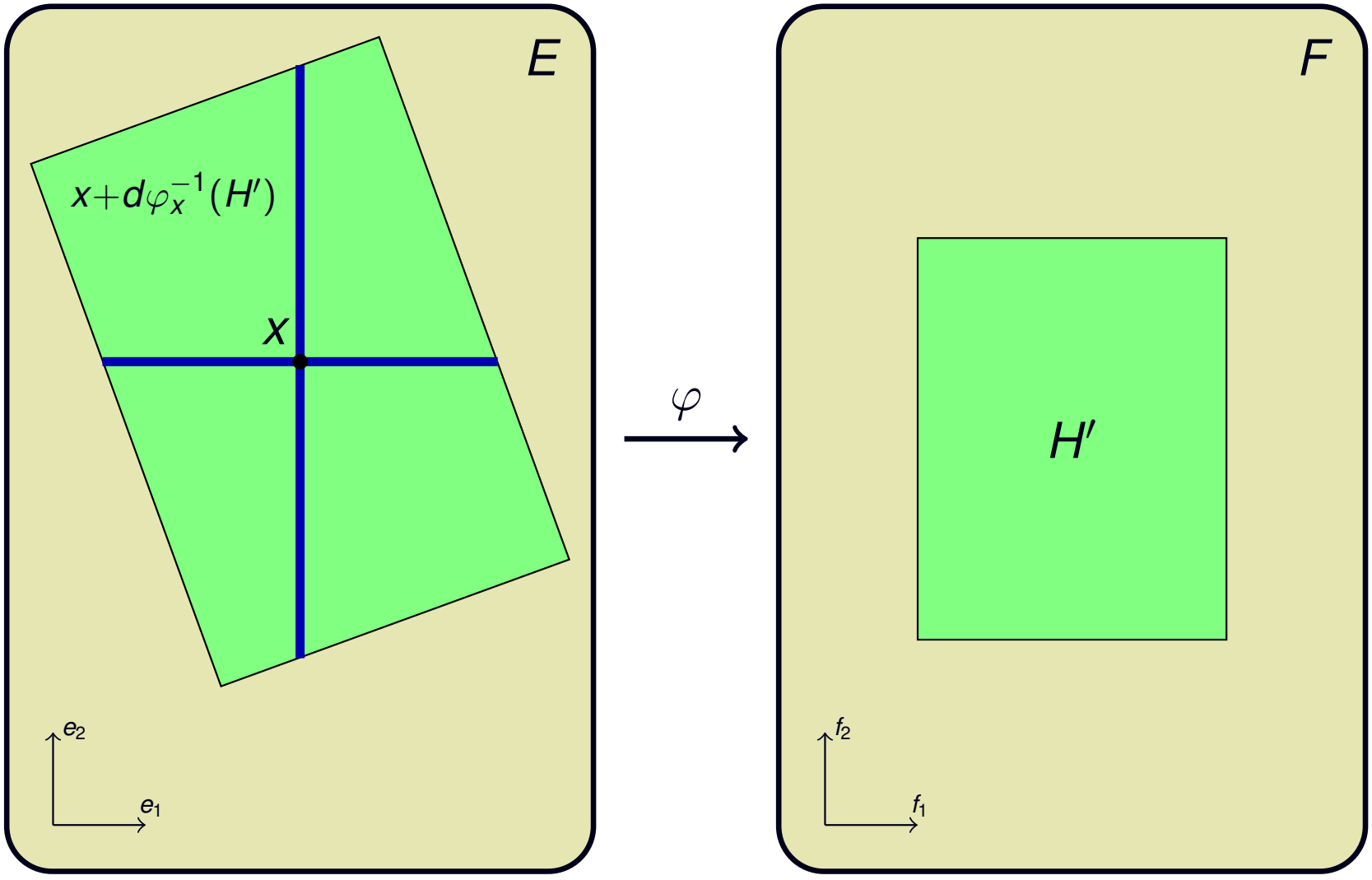
Précision optimale

Contexte de l'arithmétique paresseuse



Précision optimale

Contexte de l'arithmétique paresseuse



Précision optimale

Contexte de l’arithmétique paresseuse

Précision optimale

Contexte de l'arithmétique paresseuse

$$J(\varphi)_x \cdot \begin{pmatrix} p^{-M_1} & & \\ & \ddots & \\ & & p^{-M_m} \end{pmatrix}$$

Précision optimale

Contexte de l'arithmétique paresseuse

$$J(\varphi)_x \cdot \begin{pmatrix} p^{-M_1} & & \\ & \ddots & \\ & & p^{-M_m} \end{pmatrix} = \left(\begin{array}{c} L_1 \\ \hdashline \vdots \\ \hdashline L_n \end{array}\right)$$

Précision optimale

Contexte de l'arithmétique paresseuse

$$J(\varphi)_x \cdot \begin{pmatrix} p^{-M_1} & & \\ & \ddots & \\ & & p^{-M_m} \end{pmatrix} = \left(\begin{array}{c} L_1 \\ \hdashline \vdots \\ \hdashline L_n \end{array}\right)$$

Précision optimale requise sur la i-ième composante de x :

$$O\left(p^{-\mathrm{val}(L_i)}\right)$$

Exemple : déterminant, polynôme caractéristique

Exemple : déterminant, polynôme caractéristique

$$M = \begin{pmatrix} \ldots 0101110000 & \ldots 0011100000 & \ldots 1011001000 & \ldots 0011000100 \\ \ldots 1101011001 & \ldots 1101000111 & \ldots 0111001010 & \ldots 0101110101 \\ \ldots 0111100011 & \ldots 1011100101 & \ldots 0010100110 & \ldots 1111110111 \\ \ldots 0000111101 & \ldots 1101110011 & \ldots 0011010010 & \ldots 1001100001 \end{pmatrix}$$

Arithmétique zélée :

$$\det M = O(2^{10})$$

Arithmétique flottante :

$$\det M = 2^{10} \times \ldots 00010\mathbf{01101}$$

Arithmétique zélée :

$$\begin{aligned} \chi_M(X) = X^4 + & \quad (\ldots 0001000010)\, X^3 + \quad (\ldots 1000101100)\, X^2 \\ + & \quad (\ldots 0011100000)\, X + \quad (\ldots 0000000000) \end{aligned}$$

Arithmétique flottante :

$$\begin{aligned} \chi_M(X) = X^4 + & \quad (\ldots 0\mathbf{0001000010})\, X^3 + \quad (\ldots 11\mathbf{1000101100})\, X^2 \\ + & \, (\ldots 110\mathbf{100011100000})\, X + (2^{10} \times \ldots 00010\mathbf{01101}) \end{aligned}$$

Exemple : déterminant, polynôme caractéristique

Exemple : déterminant, polynôme caractéristique

$$\begin{array}{rccl} \varphi : & M_d(\mathbb{Q}_p) & \longrightarrow & \mathbb{Q}_p[X]_{<d} \\ & M & \mapsto & \det\left(XI_d - M\right) - X^d \end{array}$$

Exemple : déterminant, polynôme caractéristique

$$\begin{array}{rccl} \varphi : & M_d(\mathbb{Q}_p) & \longrightarrow & \mathbb{Q}_p[X]_{<d} \\ & M & \mapsto & \det\left(XI_d - M\right) - X^d \end{array}$$

Différentielle

Exemple : déterminant, polynôme caractéristique

$$\begin{array}{rccl} \varphi : & M_d(\mathbb{Q}_p) & \longrightarrow & \mathbb{Q}_p[X]_{<d} \\ & M & \mapsto & \det\left(XI_d - M\right) - X^d \end{array}$$

Différentielle

$$\det M = \sum_{j=1}^{d} (-1)^{i+j} \cdot m_{i,j} \cdot \det\ M_{i,j}$$

[developpement selon la i-ième ligne]

Exemple : déterminant, polynôme caractéristique

$$\begin{array}{rccl} \varphi : & M_d(\mathbb{Q}_p) & \longrightarrow & \mathbb{Q}_p[X]_{<d} \\ & M & \mapsto & \det\left(XI_d - M\right) - X^d \end{array}$$

Différentielle

$$\det M = \sum_{j=1}^{d} (-1)^{i+j} \cdot m_{i,j} \cdot \det\ M_{i,j}$$

[developpement selon la i-ième ligne]

$$\Longrightarrow \quad \frac{\partial \det}{\partial x_{i,j}}(M) = (-1)^{i+j} \cdot \det\ M_{i,j}$$

Exemple : déterminant, polynôme caractéristique

$$\begin{array}{rccc} \varphi : & M_d(\mathbb{Q}_p) & \longrightarrow & \mathbb{Q}_p[X]_{<d} \\ & M & \mapsto & \det\left(XI_d - M\right) - X^d \end{array}$$

Différentielle

$$\det M = \sum_{j=1}^{d} (-1)^{i+j} \cdot m_{i,j} \cdot \det\ M_{i,j}$$

[developpement selon la i-ième ligne]

$$\Longrightarrow \quad \frac{\partial \det}{\partial x_{i,j}}(M) = (-1)^{i+j} \cdot \det\ M_{i,j}$$

$$\Longrightarrow \quad \frac{\partial \varphi}{\partial x_{i,j}}(M) = (-1)^{i+j} \cdot \det\left(XI_d - M\right)_{i,j}$$

Exemple : déterminant, polynôme caractéristique

$$M = \begin{pmatrix} \ldots 0101110000 & \ldots 0011100000 & \ldots 1011001000 & \ldots 0011000100 \\ \ldots 1101011001 & \ldots 1101000111 & \ldots 0111001010 & \ldots 0101110101 \\ \ldots 0111100011 & \ldots 1011100101 & \ldots 0010100110 & \ldots 1111110111 \\ \ldots 0000111101 & \ldots 1101110011 & \ldots 0011010010 & \ldots 1001100001 \end{pmatrix}$$

Exemple : déterminant, polynôme caractéristique

$$M = \begin{pmatrix} \ldots 0101110000 & \ldots 0011100000 & \ldots 1011001000 & \ldots 0011000100 \\ \ldots 1101011001 & \ldots 1101000111 & \ldots 0111001010 & \ldots 0101110101 \\ \ldots 0111100011 & \ldots 1011100101 & \ldots 0010100110 & \ldots 1111110111 \\ \ldots 0000111101 & \ldots 1101110011 & \ldots 0011010010 & \ldots 1001100001 \end{pmatrix}$$

$$\begin{array}{c} (i,j) \\ (1,1) \\ (1,2) \\ (1,3) \\ (1,4) \\ (2,1) \\ (2,2) \\ (2,3) \\ (2,4) \\ (3,1) \\ (3,2) \\ (3,3) \\ (3,4) \\ (4,1) \\ (4,2) \\ (4,3) \\ (4,4) \end{array} \begin{array}{c} X^3 \\ \left(\begin{array}{c} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{array} \right. \end{array} \begin{array}{c} X^2 \\ \begin{array}{c} \ldots 0110110010 \\ \ldots 0011100000 \\ \ldots 1011001000 \\ \ldots 0011000100 \\ \ldots 1101011001 \\ \ldots 1110001001 \\ \ldots 0111001010 \\ \ldots 0101110101 \\ \ldots 0111100011 \\ \ldots 1011100101 \\ \ldots 0011101000 \\ \ldots 1111110111 \\ \ldots 0000111101 \\ \ldots 1101110011 \\ \ldots 0011010010 \\ \ldots 1010100011 \end{array} \end{array} \begin{array}{c} X \\ \begin{array}{c} \ldots 0111111000 \\ \ldots 1011010100 \\ \ldots 1001001000 \\ \ldots 1111100100 \\ \ldots 1010010000 \\ \ldots 1001001100 \\ \ldots 0110011000 \\ \ldots 0111111100 \\ \ldots 1010000000 \\ \ldots 1110100000 \\ \ldots 1001000100 \\ \ldots 1111100100 \\ \ldots 0010111000 \\ \ldots 1101011000 \\ \ldots 1101001000 \\ \ldots 0111010000 \end{array} \end{array} \begin{array}{c} 1 \\ \left(\begin{array}{c} \ldots 0001000000 \\ \ldots 1110100000 \\ \ldots 0011000000 \\ \ldots 0110100000 \\ \ldots 1001000000 \\ \ldots 1100100000 \\ \ldots 0111000000 \\ \ldots 0100100000 \\ \ldots 1001000000 \\ \ldots 1110100000 \\ \ldots 1001000000 \\ \ldots 1100100000 \\ \ldots 0110000000 \\ \ldots 1001000000 \\ \ldots 0010000000 \\ \ldots 1101000000 \end{array} \right. \end{array} = J(\varphi)_M$$

Exemple : déterminant, polynôme caractéristique

$$M = \begin{pmatrix} \ldots 0101110000 & \ldots 0011100000 & \ldots 1011001000 & \ldots 0011000100 \\ \ldots 1101011001 & \ldots 1101000111 & \ldots 0111001010 & \ldots 0101110101 \\ \ldots 0111100011 & \ldots 1011100101 & \ldots 0010100110 & \ldots 1111110111 \\ \ldots 0000111101 & \ldots 1101110011 & \ldots 0011010010 & \ldots 1001100001 \end{pmatrix}$$

Arithmétique zélée :

$$\det M = O(2^{10})$$

Arithmétique flottante :

$$\det M = 2^{10} \times \ldots 00010\mathbf{01101}$$

Arithmétique zélée :

$$\begin{aligned} \chi_M(X) = X^4 + & \quad (\ldots 0001000010)\, X^3 + \quad (\ldots 1000101100)\, X^2 \\ + & \quad (\ldots 0011100000)\, X + \quad (\ldots 0000000000) \end{aligned}$$

Arithmétique flottante :

$$\begin{aligned} \chi_M(X) = X^4 + & \quad (\ldots 0\mathbf{0001000010})\, X^3 + \quad (\ldots 11\mathbf{1000101100})\, X^2 \\ + & \, (\ldots 110\mathbf{1000011100000})\, X + (2^{10} \times \ldots 00010\mathbf{01101}) \end{aligned}$$

Exemple : factorisation LU

Exemple : factorisation LU

$$M = \begin{pmatrix} \ldots 0101110000 & \ldots 0011100000 & \ldots 1011001000 & \ldots 0011000100 \\ \ldots 1101011001 & \ldots 1101000111 & \ldots 0111001010 & \ldots 0101110101 \\ \ldots 0111100011 & \ldots 1011100101 & \ldots 0010100110 & \ldots 1111110111 \\ \ldots 0000111101 & \ldots 1101110011 & \ldots 0011010010 & \ldots 1001100001 \end{pmatrix}$$

Arithmétique zélée :

$$L = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2^{-4} \times \ldots 001111 & 1 & 0 & 0 \\ 2^{-4} \times \ldots 010101 & \ldots 100011 & 1 & 0 \\ 2^{-4} \times \ldots 001011 & \ldots 010101 & \ldots 110 & 1 \end{pmatrix}$$

Arithmétique flottante :

$$L = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2^{-4} \times \ldots 1010001111 & 1 & 0 & 0 \\ 2^{-4} \times \ldots 0110010101 & \ldots 0011100011 & 1 & 0 \\ 2^{-4} \times \ldots 0101001011 & \ldots 0111010101 & 00010110110 & 1 \end{pmatrix}$$

Exemple : factorisation LU

Exemple : factorisation LU

$$\begin{array}{rccl} \varphi : & M_d(\mathbb{Q}_p) & \longrightarrow & L_d(\mathbb{Q}_p) \\ & M & \mapsto & L - I_d \quad \text{t.q.} \quad M = LU \end{array}$$

Exemple : factorisation LU

$$\begin{array}{rccc} \varphi : & M_d(\mathbb{Q}_p) & \longrightarrow & L_d(\mathbb{Q}_p) \\ & M & \mapsto & L - I_d \quad \text{t.q.} \quad M = LU \end{array}$$

Différentielle

Exemple : factorisation LU

$$\begin{array}{rccl} \varphi : & M_d(\mathbb{Q}_p) & \longrightarrow & L_d(\mathbb{Q}_p) \\ & M & \mapsto & L - I_d \quad \text{t.q.} \quad M = LU \end{array}$$

Différentielle

$$M = LU$$

Exemple : factorisation LU

$$\begin{array}{rccl} \varphi : & M_d(\mathbb{Q}_p) & \longrightarrow & L_d(\mathbb{Q}_p) \\ & M & \mapsto & L - I_d \quad \text{t.q.} \quad M = LU \end{array}$$

Différentielle

$$M = LU$$

$$dM = dL \cdot U + L \cdot dU$$

Exemple : factorisation LU

$$\begin{array}{rccl} \varphi : & M_d(\mathbb{Q}_p) & \longrightarrow & L_d(\mathbb{Q}_p) \\ & M & \mapsto & L - I_d \quad \text{t.q.} \quad M = LU \end{array}$$

Différentielle

$$M = LU$$

$$dM = dL \cdot U + L \cdot dU$$

$$L^{-1} \cdot dM \cdot U^{-1} = L^{-1} \cdot dL + dU \cdot U^{-1}$$

Exemple : factorisation LU

$$\begin{array}{rccl} \varphi : & M_d(\mathbb{Q}_p) & \longrightarrow & L_d(\mathbb{Q}_p) \\ & M & \mapsto & L - I_d \quad \text{t.q.} \quad M = LU \end{array}$$

Différentielle

$$\begin{aligned} M &= LU \\ dM &= dL \cdot U + L \cdot dU \\ L^{-1} \cdot dM \cdot U^{-1} &= L^{-1} \cdot dL + dU \cdot U^{-1} \\ \mathrm{Low}\left(L^{-1} \cdot dM \cdot U^{-1}\right) &= L^{-1} \cdot dL \\ \mathrm{Upp}\left(L^{-1} \cdot dM \cdot U^{-1}\right) &= dU \cdot U^{-1} \end{aligned}$$

Exemple : factorisation LU

$$\begin{array}{rccl} \varphi : & M_d(\mathbb{Q}_p) & \longrightarrow & L_d(\mathbb{Q}_p) \\ & M & \mapsto & L - I_d \quad \text{t.q.} \quad M = LU \end{array}$$

Différentielle

$$M = LU$$

$$dM = dL \cdot U + L \cdot dU$$

$$L^{-1} \cdot dM \cdot U^{-1} = L^{-1} \cdot dL + dU \cdot U^{-1}$$

$$\begin{aligned} \mathrm{Low}\left(L^{-1} \cdot dM \cdot U^{-1}\right) &= L^{-1} \cdot dL \\ \mathrm{Upp}\left(L^{-1} \cdot dM \cdot U^{-1}\right) &= dU \cdot U^{-1} \end{aligned}$$

$$\Longrightarrow \quad d\varphi_M : \, dM \mapsto dL = L \cdot \mathrm{Lo}\left(L^{-1} \cdot dM \cdot U^{-1}\right) \quad \text{si } M = LU$$

Exemple : factorisation LU

$$M = \begin{pmatrix} \ldots 0101110000 & \ldots 0011100000 & \ldots 1011001000 & \ldots 0011000100 \\ \ldots 1101011001 & \ldots 1101000111 & \ldots 0111001010 & \ldots 0101110101 \\ \ldots 0111100011 & \ldots 1011100101 & \ldots 0010100110 & \ldots 1111110111 \\ \ldots 0000111101 & \ldots 1101110011 & \ldots 0011010010 & \ldots 1001100001 \end{pmatrix}$$

Exemple : factorisation LU

$$M = \begin{pmatrix} \ldots 0101110000 & \ldots 0011100000 & \ldots 1011001000 & \ldots 0011000100 \\ \ldots 1101011001 & \ldots 1101000111 & \ldots 0111001010 & \ldots 0101110101 \\ \ldots 0111100011 & \ldots 1011100101 & \ldots 0010100110 & \ldots 1111110111 \\ \ldots 0000111101 & \ldots 1101110011 & \ldots 0011010010 & \ldots 1001100001 \end{pmatrix}$$

$$\begin{array}{c} \\ (1,1) \\ (1,2) \\ (1,3) \\ (1,4) \\ (2,1) \\ (2,2) \\ (2,3) \\ (2,4) \\ (3,1) \\ (3,2) \\ (3,3) \\ (3,4) \\ (4,1) \\ (4,2) \\ (4,3) \\ (4,4) \end{array} \begin{array}{c} \begin{array}{ccc} (3,2) & (4,2) & (4,3) \end{array} \\ \begin{pmatrix} \ldots 1100101 & \ldots 1100010 & \ldots 001{,}01 \\ \ldots 110101{,}1 & \ldots 011111 & \ldots 100{,}01 \\ 0 & 0 & \ldots 1011{,}1 \\ 0 & 0 & 0 \\ \ldots 0111001110 & \ldots 11100010 & \ldots 0110{,}111 \\ \ldots 0100001001 & \ldots 0011111 & \ldots 1111{,}011 \\ 0 & 0 & \ldots 10111{,}01 \\ 0 & 0 & 0 \\ \ldots 00110100110 & \ldots 00000000 & \ldots 1111{,}11 \\ \ldots 0111011101 & \ldots 0000000 & \ldots 1000{,}11 \\ 0 & 0 & \ldots 11010{,}1 \\ 0 & 0 & 0 \\ 0 & \ldots 00110100110 & \ldots 1010{,}011 \\ 0 & \ldots 0111011101 & \ldots 0100{,}111 \\ 0 & 0 & \ldots 00100{,}01 \\ 0 & 0 & 0 \end{pmatrix} \end{array} = J(\varphi)_M$$

Exemple : factorisation LU

$$M = \begin{pmatrix} \ldots 0101110000 & \ldots 0011100000 & \ldots 1011001000 & \ldots 0011000100 \\ \ldots 1101011001 & \ldots 1101000111 & \ldots 0111001010 & \ldots 0101110101 \\ \ldots 0111100011 & \ldots 1011100101 & \ldots 0010100110 & \ldots 1111110111 \\ \ldots 0000111101 & \ldots 1101110011 & \ldots 0011010010 & \ldots 1001100001 \end{pmatrix}$$

Arithmétique zélée :

$$L = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2^{-4} \times \ldots 001111 & 1 & 0 & 0 \\ 2^{-4} \times \ldots 010101 & \ldots 100011 & 1 & 0 \\ 2^{-4} \times \ldots 001011 & \ldots 010101 & \ldots 110 & 1 \end{pmatrix}$$

Arithmétique flottante :

$$L = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2^{-4} \times \ldots 1010001111 & 1 & 0 & 0 \\ 2^{-4} \times \ldots 0110010101 & \ldots 0011100011 & 1 & 0 \\ 2^{-4} \times \ldots 0101001011 & \ldots 0111010101 & 00010110110 & 1 \end{pmatrix}$$

Exemple : coefficients de Bézout

Exemple : coefficients de Bézout

$$P = X^4 + (\ldots 1101111111)\, X^3 + (\ldots 0011110011)\, X^2 + (\ldots 1001001100)\, X + (\ldots 0010111010)$$

$$Q = X^4 + (\ldots 0101001011)\, X^3 + (\ldots 0111001111)\, X^2 + (\ldots 0100010000)\, X + (\ldots 1101000111)$$

Arithmétique zélée :

$$U = (\ldots 101100)\, X^3 + (\ldots 101100)\, X^2 + (\ldots 100)\, X + (\ldots 1011)$$

$$V = (\ldots 010100)\, X^3 + (\ldots 100100)\, X^2 + (\ldots 100)\, X + (\ldots 101)$$

Arithmétique flottante :

$$U = (\ldots 101011101100)\, X^3 + (\ldots 111100101100)\, X^2 + (\ldots 100000110100)\, X + (\ldots 0110001011)$$

$$V = (\ldots 010100010100)\, X^3 + (\ldots 001011100100)\, X^2 + (\ldots 000100111100)\, X + (\ldots 1111100101)$$

Exemple : coefficients de Bézout

Exemple : coefficients de Bézout

$$\begin{array}{rccl} \varphi : & \left(\mathbb{Q}_p[X]_{<d}\right)^2 & \longrightarrow & \left(\mathbb{Q}_p[X]_{<d}\right)^2 \\ & (\tilde{P}, \tilde{Q}) & \mapsto & (U, V) \\ & & & \text{t.q.} \quad U\cdot(X^d+\tilde{P}) + V\cdot(X^d+\tilde{Q}) = 1 \end{array}$$

Exemple : coefficients de Bézout

$$\begin{array}{rccl} \varphi : & \left(\mathbb{Q}_p[X]_{<d}\right)^2 & \longrightarrow & \left(\mathbb{Q}_p[X]_{<d}\right)^2 \\ & (\tilde{P}, \tilde{Q}) & \mapsto & (U, V) \\ & & & \text{t.q.} \quad U\cdot(X^d+\tilde{P}) + V\cdot(X^d+\tilde{Q}) = 1 \end{array}$$

Différentielle

Exemple : coefficients de Bézout

$$\begin{array}{rccl} \varphi : & \left(\mathbb{Q}_p[X]_{<d}\right)^2 & \longrightarrow & \left(\mathbb{Q}_p[X]_{<d}\right)^2 \\ & (\tilde{P}, \tilde{Q}) & \mapsto & (U, V) \\ & & & \text{t.q.} \quad U\cdot(X^d+\tilde{P}) + V\cdot(X^d+\tilde{Q}) = 1 \end{array}$$

Différentielle

$$UP + VQ = 1$$

Exemple : coefficients de Bézout

$$\begin{array}{rccl} \varphi : & \left(\mathbb{Q}_p[X]_{<d}\right)^2 & \longrightarrow & \left(\mathbb{Q}_p[X]_{<d}\right)^2 \\ & (\tilde{P}, \tilde{Q}) & \mapsto & (U, V) \\ & & & \text{t.q.} \quad U\cdot(X^d+\tilde{P}) + V\cdot(X^d+\tilde{Q}) = 1 \end{array}$$

Différentielle

$$UP + VQ = 1$$

$$dU\cdot P + dV\cdot Q = -(U\cdot dP + V\cdot dQ)$$

Exemple : coefficients de Bézout

$$\begin{array}{rccl} \varphi : & \left(\mathbb{Q}_p[X]_{<d}\right)^2 & \longrightarrow & \left(\mathbb{Q}_p[X]_{<d}\right)^2 \\ & (\tilde{P}, \tilde{Q}) & \mapsto & (U, V) \\ & & & \text{t.q.} \quad U\cdot(X^d+\tilde{P}) + V\cdot(X^d+\tilde{Q}) = 1 \end{array}$$

Différentielle

$$\begin{aligned} UP + VQ &= 1 \\ dU\cdot P + dV\cdot Q &= -(U\cdot dP + V\cdot dQ) \\ dU &= -U\cdot(U\cdot dP + V\cdot dQ) \bmod Q \end{aligned}$$

Exemple : coefficients de Bézout

$$\begin{array}{rccl} \varphi : & \left(\mathbb{Q}_p[X]_{<d}\right)^2 & \longrightarrow & \left(\mathbb{Q}_p[X]_{<d}\right)^2 \\ & (\tilde{P}, \tilde{Q}) & \mapsto & (U, V) \\ & & & \text{t.q.} \quad U\cdot(X^d+\tilde{P}) + V\cdot(X^d+\tilde{Q}) = 1 \end{array}$$

Différentielle

$$UP + VQ = 1$$

$$dU\cdot P + dV\cdot Q = -(U\cdot dP + V\cdot dQ)$$

$$dU = -U\cdot(U\cdot dP + V\cdot dQ) \mod Q$$

$$dV = -V\cdot(U\cdot dP + V\cdot dQ) \mod P$$

Exemple : coefficients de Bézout

$$\begin{array}{rccl} \varphi : & \left(\mathbb{Q}_p[X]_{<d}\right)^2 & \longrightarrow & \left(\mathbb{Q}_p[X]_{<d}\right)^2 \\ & (\tilde{P}, \tilde{Q}) & \mapsto & (U, V) \\ & & & \text{t.q.} \quad U\cdot(X^d+\tilde{P}) + V\cdot(X^d+\tilde{Q}) = 1 \end{array}$$

Différentielle

$$UP + VQ = 1$$

$$dU\cdot P + dV\cdot Q = -(U\cdot dP + V\cdot dQ)$$

$$dU = -U\cdot(U\cdot dP + V\cdot dQ) \mod Q$$

$$dV = -V\cdot(U\cdot dP + V\cdot dQ) \mod P$$

$$\Longrightarrow \quad d\varphi_{(\tilde{P},\tilde{Q})} : (dP, dQ) \mapsto (U\cdot dR \mod Q,\ V\cdot dR \mod P)$$

$$\text{si } UP + VQ = 1,\ dR = -U\cdot dP - V\cdot dQ$$

Exemple : coefficients de Bézout

$$P = X^4 + (\ldots 1101111111)\, X^3 + (\ldots 0011110011)\, X^2 + (\ldots 1001001100)\, X + (\ldots 0010111010)$$

$$Q = X^4 + (\ldots 0101001011)\, X^3 + (\ldots 0111001111)\, X^2 + (\ldots 0100010000)\, X + (\ldots 1101000111)$$

Exemple : coefficients de Bézout

$$P = X^4 + (\ldots 1101111111)\, X^3 + (\ldots 0011110011)\, X^2 + (\ldots 1001001100)\, X + (\ldots 0010111010)$$

$$Q = X^4 + (\ldots 0101001011)\, X^3 + (\ldots 0111001111)\, X^2 + (\ldots 0100010000)\, X + (\ldots 1101000111)$$

$$\begin{array}{c} \\ (dP, dQ) \\ (X^3, 0) \\ (X^2, 0) \\ (X, 0) \\ (1, 0) \\ \\ (0, X^3) \\ (0, X^2) \\ (0, X) \\ (0, 1) \end{array} \begin{array}{c} \\ X^3 \\ \ldots 0100111 \\ \ldots 1010000 \\ \ldots 1000000 \\ \ldots 1111000 \\ \\ \ldots 1011001 \\ \ldots 1110000 \\ \ldots 0010000 \\ \ldots 1001000 \end{array} \begin{array}{c} dU \\ X^2 \\ \ldots 0001000 \\ \ldots 0010111 \\ \ldots 0010000 \\ \ldots 1101000 \\ \\ \ldots 1111000 \\ \ldots 0101001 \\ \ldots 0100000 \\ \ldots 0101000 \end{array} \begin{array}{c} \\ X \\ \ldots 1000000 \\ \ldots 0111000 \\ \ldots 1010111 \\ \ldots 0011000 \\ \\ \ldots 0010000 \\ \ldots 0001000 \\ \ldots 0011001 \\ \ldots 1011000 \end{array} \begin{array}{c} \\ 1 \\ \ldots 1010000 \\ \ldots 1000000 \\ \ldots 0111000 \\ \ldots 1010111 \\ \\ \ldots 1110000 \\ \ldots 0010000 \\ \ldots 0001000 \\ \ldots 0011001 \end{array} = J(\varphi)_{(\tilde{P}, \tilde{Q})}$$

Exemple : coefficients de Bézout

$$P = X^4 + (\ldots 1101111111)\, X^3 + (\ldots 0011110011)\, X^2 + (\ldots 1001001100)\, X + (\ldots 0010111010)$$

$$Q = X^4 + (\ldots 0101001011)\, X^3 + (\ldots 0111001111)\, X^2 + (\ldots 0100010000)\, X + (\ldots 1101000111)$$

$$\begin{array}{c} \\ (dP, dQ) \\ (X^3, 0) \\ (X^2, 0) \\ (X, 0) \\ (1, 0) \\ \\ (0, X^3) \\ (0, X^2) \\ (0, X) \\ (0, 1) \end{array} \begin{array}{c} \\ X^3 \\ \ldots 1011001 \\ \ldots 0110000 \\ \ldots 1000000 \\ \ldots 0001000 \\ \\ \ldots 0100111 \\ \ldots 0010000 \\ \ldots 1110000 \\ \ldots 0111000 \end{array} \begin{array}{c} dV \\ X^2 \\ \ldots 0100000 \\ \ldots 0101001 \\ \ldots 1110000 \\ \ldots 0111000 \\ \\ \ldots 1100000 \\ \ldots 0010111 \\ \ldots 0100000 \\ \ldots 0111000 \end{array} \begin{array}{c} \\ X \\ \ldots 1000000 \\ \ldots 0110000 \\ \ldots 1101001 \\ \ldots 0001000 \\ \\ \ldots 1100000 \\ \ldots 0010000 \\ \ldots 1100111 \\ \ldots 1001000 \end{array} \begin{array}{c} \\ 1 \\ \ldots 0100000 \\ \ldots 0000000 \\ \ldots 0110000 \\ \ldots 1001001 \\ \\ \ldots 1100000 \\ \ldots 0100000 \\ \ldots 1010000 \\ \ldots 0000111 \end{array} = J(\varphi)_{(\tilde{P}, \tilde{Q})}$$

Exemple : coefficients de Bézout

$$P = X^4 + (\ldots 1101111111)\, X^3 + (\ldots 0011110011)\, X^2 + (\ldots 1001001100)\, X + (\ldots 0010111010)$$

$$Q = X^4 + (\ldots 0101001011)\, X^3 + (\ldots 0111001111)\, X^2 + (\ldots 0100010000)\, X + (\ldots 1101000111)$$

Arithmétique zélée :

$$U = (\ldots 101100)\, X^3 + (\ldots 101100)\, X^2 + (\ldots 100)\, X + (\ldots 1011)$$

$$V = (\ldots 010100)\, X^3 + (\ldots 100100)\, X^2 + (\ldots 100)\, X + (\ldots 101)$$

Arithmétique flottante :

$$U = (\ldots 101011101100)\, X^3 + (\ldots 111100101100)\, X^2 + (\ldots 100000110100)\, X + (\ldots 01110001011)$$

$$V = (\ldots 010100010100)\, X^3 + (\ldots 001011100100)\, X^2 + (\ldots 000100111100)\, X + (\ldots 1111100101)$$

Exemple : évaluation et interpolation

Exemple : évaluation et interpolation

$$
\begin{aligned}
P = {} & (\ldots 0101101001)\, X^{19} + (\ldots 1101000011)\, X^{18} + (\ldots 0011001110)\, X^{17} + (\ldots 1001011010)\, X^{16} \\
& + (\ldots 0011100111)\, X^{15} + (\ldots 0110101110)\, X^{14} + (\ldots 0111111001)\, X^{13} + (\ldots 1011010111)\, X^{12} \\
& + (\ldots 0100000100)\, X^{11} + (\ldots 0000110000)\, X^{10} + (\ldots 1110101010)\, X^{9} + (\ldots 1111101100)\, X^{8} \\
& + (\ldots 0100010001)\, X^{7} + (\ldots 0101010000)\, X^{6} + (\ldots 0111101111)\, X^{5} + (\ldots 1100010011)\, X^{4} \\
& + (\ldots 0100000001)\, X^{3} + (\ldots 1000010010)\, X^{2} + (\ldots 0000100000)\, X + (\ldots 0001111110)
\end{aligned}
$$

Arithmétique zélée :

$$
\begin{aligned}
& O(2^{-6})\, X^{19} + O(2^{-6})\, X^{18} + O(2^{-6})\, X^{17} \\
+ \; & O(2^{-5})\, X^{16} + O(2^{-6})\, X^{15} + O(2^{-6})\, X^{14} \\
+ \; & O(2^{-6})\, X^{13} + O(2^{-5})\, X^{12} + O(2^{-6})\, X^{11} \\
+ \; & O(2^{-6})\, X^{10} + O(2^{-6})\, X^{9} + O(2^{-5})\, X^{8} \\
+ \; & O(2^{-4})\, X^{7} + O(2^{-3})\, X^{6} + O(2^{-2})\, X^{5} \\
+ \; & O(2^{-1})\, X^{4} + (\ldots 1)\, X^{3} + (\ldots 010)\, X^{2} \\
+ \; & (\ldots 100000)\, X + (\ldots 0001111110)
\end{aligned}
$$

Arithmétique flottante :

$$
\begin{aligned}
& (2^{-3} \times \ldots 1110011011)\, X^{19} + (2^{-5} \times \ldots 0000000011)\, X^{18} + (2^{-3} \times \ldots 0001011111)\, X^{17} \\
+ \; & (2^{-5} \times \ldots 1100111101)\, X^{16} + (\ldots 11111100110)\, X^{15} + (2^{-4} \times \ldots 0110100011)\, X^{14} \\
+ \; & (2^{-2} \times \ldots 0000010011)\, X^{13} + (2^{-4} \times \ldots 1010001101)\, X^{12} + (2^{-3} \times \ldots 0010000011)\, X^{11} \\
+ \; & (2^{-5} \times \ldots 0100101111)\, X^{10} + (2^{-3} \times \ldots 0000110011)\, X^{9} + (2^{-5} \times \ldots 1010101001)\, X^{8} \\
+ \; & (2^{-2} \times \ldots 0010000101)\, X^{7} + (2^{-2} \times \ldots 1101100111)\, X^{6} + (\ldots 1101101111)\, X^{5} \\
+ \; & (2^{-1} \times \ldots 0011100111)\, X^{4} + (\ldots 0101110101)\, X^{3} + (\ldots 1101110101010)\, X^{2} \\
+ \; & (\ldots 000000001100000)\, X + (\ldots 000001111110)
\end{aligned}
$$

Exemple : évaluation et interpolation

Exemple : évaluation et interpolation

$$\begin{array}{rccc} \varphi : & \mathbb{Q}_p[X]_{<d} & \longrightarrow & \mathbb{Q}_p^d \\ & P & \mapsto & \big(P(1), P(2), \ldots, P(d)\big) \end{array}$$

Exemple : évaluation et interpolation

$$\begin{array}{rccc} \varphi : & \mathbb{Q}_p[X]_{<d} & \longrightarrow & \mathbb{Q}_p^d \\ & P & \mapsto & \big(P(1), P(2), \ldots, P(d)\big) \end{array}$$

Différentielle

Exemple : évaluation et interpolation

$$\begin{array}{rccc} \varphi : & \mathbb{Q}_p[X]_{<d} & \longrightarrow & \mathbb{Q}_p^d \\ & P & \mapsto & \big(P(1), P(2), \ldots, P(d)\big) \end{array}$$

Différentielle

φ est linéaire

Exemple : évaluation et interpolation

$$\begin{array}{rccc} \varphi : & \mathbb{Q}_p[X]_{<d} & \longrightarrow & \mathbb{Q}_p^d \\ & P & \mapsto & \big(P(1), P(2), \ldots, P(d)\big) \end{array}$$

Différentielle

φ est linéaire :

$$J(\varphi) = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 2 & \cdots & 2^{d-1} \\ 1 & 3 & \cdots & 3^{d-1} \\ \vdots & \vdots & & \vdots \\ 1 & d & \cdots & d^{d-1} \end{pmatrix}$$

$$\det J(\varphi) = 1! \times 2! \times \cdots \times d!$$

Exemple : évaluation et interpolation

$$\begin{array}{rccc} \varphi : & \mathbb{Q}_p[X]_{<d} & \longrightarrow & \mathbb{Q}_p^d \\ & P & \mapsto & \big(P(1), P(2), \ldots, P(d)\big) \end{array}$$

Différentielle

φ est linéaire :

$$J(\varphi) = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 2 & \cdots & 2^{d-1} \\ 1 & 3 & \cdots & 3^{d-1} \\ \vdots & \vdots & & \vdots \\ 1 & d & \cdots & d^{d-1} \end{pmatrix}$$

$$\det J(\varphi) = 1! \times 2! \times \cdots \times d!$$

$$\Longrightarrow \quad \mathrm{val}_p(1! \times 2! \times \cdots \times d!) \geq \tfrac{d^2}{2p} \quad \text{chiffres de précision diffus}$$

Exemple : évaluation et interpolation

$$
\begin{aligned}
P = {} & (\ldots 0101101001)\, X^{19} + (\ldots 1101000011)\, X^{18} + (\ldots 0011001110)\, X^{17} + (\ldots 1001011010)\, X^{16} \\
& + (\ldots 0011100111)\, X^{15} + (\ldots 0110101110)\, X^{14} + (\ldots 0111111001)\, X^{13} + (\ldots 1011010111)\, X^{12} \\
& + (\ldots 0100000100)\, X^{11} + (\ldots 0000110000)\, X^{10} + (\ldots 1110101010)\, X^{9} + (\ldots 1111101100)\, X^{8} \\
& + (\ldots 0100010001)\, X^{7} + (\ldots 0101010000)\, X^{6} + (\ldots 0111101111)\, X^{5} + (\ldots 1100010011)\, X^{4} \\
& + (\ldots 0100000001)\, X^{3} + (\ldots 1000010010)\, X^{2} + (\ldots 0000100000)\, X + (\ldots 0001111110)
\end{aligned}
$$

Arithmétique zélée :

$$
\begin{aligned}
& O(2^{-6})\, X^{19} + && O(2^{-6})\, X^{18} + && O(2^{-6})\, X^{17} \\
+ \; & O(2^{-5})\, X^{16} + && O(2^{-6})\, X^{15} + && O(2^{-6})\, X^{14} \\
+ \; & O(2^{-6})\, X^{13} + && O(2^{-5})\, X^{12} + && O(2^{-6})\, X^{11} \\
+ \; & O(2^{-6})\, X^{10} + && O(2^{-6})\, X^{9} + && O(2^{-5})\, X^{8} \\
+ \; & O(2^{-4})\, X^{7} + && O(2^{-3})\, X^{6} + && O(2^{-2})\, X^{5} \\
+ \; & O(2^{-1})\, X^{4} + && (\ldots 1)\, X^{3} + && (\ldots 010)\, X^{2} \\
+ \; & (\ldots 100000)\, X + && (\ldots 0001111110) &&
\end{aligned}
$$

Arithmétique flottante :

$$
\begin{aligned}
& (2^{-3} \times \ldots 1110011011)\, X^{19} + (2^{-5} \times \ldots 0000000011)\, X^{18} + (2^{-3} \times \ldots 0001011111)\, X^{17} \\
+ \; & (2^{-5} \times \ldots 1100111101)\, X^{16} + && (\ldots 11111100110)\, X^{15} + (2^{-4} \times \ldots 0110100011)\, X^{14} \\
+ \; & (2^{-2} \times \ldots 0000010011)\, X^{13} + (2^{-4} \times \ldots 1010001101)\, X^{12} + (2^{-3} \times \ldots 0010000011)\, X^{11} \\
+ \; & (2^{-5} \times \ldots 0100101111)\, X^{10} + (2^{-3} \times \ldots 0000110011)\, X^{9} + (2^{-5} \times \ldots 1010101001)\, X^{8} \\
+ \; & (2^{-2} \times \ldots 0010000101)\, X^{7} + (2^{-2} \times \ldots 1101100111)\, X^{6} + && (\ldots 1101101111)\, X^{5} \\
+ \; & (2^{-1} \times \ldots 0011100111)\, X^{4} + && (\ldots 0101110101)\, X^{3} + && (\ldots 1101110101 0)\, X^{2} \\
+ \; & (\ldots 0000000011 00000)\, X + && (\ldots 0000111111 0) &&
\end{aligned}
$$

Itération de Newton

Itération de Newton

Théorème

Soit $f : B_E(1) \to F$ une fonction de classe C^2.

Soit $a \in \mathbb{Z}_p$ tel que :

$$\|f(a)\| < \frac{\|df_a\|^2}{\|d^2 f\|_\infty} \quad \text{et} \quad \|f(a)\| < \|df_a\|.$$

Alors, la suite récurrente définie par

$$x_0 = a \quad ; \quad x_{i+1} = x_i - df_{x_i}^{-1}\big(f(x_i)\big)$$

converge vers un zéro de f.

C'est le seul dans la boule de centre a et de rayon $\dfrac{\|df_a\|}{\|f''\|_\infty}$.

Itération de Newton

Objectif

Calcul de $\sqrt{\ldots 11110010010000111001}$

Schéma de Newton

$$x_0 = 1 \quad ; \quad x_{i+1} = \frac{1}{2}\left(x_i + \frac{c}{x_i}\right)$$

Résultats

$$\begin{aligned}
x_1 &: \quad \ldots 00000000000000000101 \\
x_2 &: \quad \ldots 00000000000000010101 \\
x_3 &: \quad \ldots 00000000000001010101 \\
x_4 &: \quad \ldots 00010111010001010101 \\
x_5 &: \quad \ldots 10101110100010101010 \\
x_6 &: \quad \ldots 10101110100010101010
\end{aligned}$$

Itération de Newton

Itération de Newton

$\mathcal{U}$ — ouvert (d'un sous-ev) de $C^2(B_E(1), F)$

Itération de Newton

$\mathcal{U}$ — ouvert (d'un sous-ev) de $C^2(B_E(1), F)$

$$\begin{array}{rccc} \mathcal{Z}: & \mathcal{U} & \longrightarrow & V \\ & f & \mapsto & x \quad \text{t.q.} \quad f(x) = 0 \end{array}$$

Itération de Newton

$\mathcal{U}$ — ouvert (d'un sous-ev) de $C^2(B_E(1), F)$

$$\begin{array}{rccc} \mathcal{Z}: & \mathcal{U} & \longrightarrow & V \\ & f & \mapsto & x \quad \text{t.q.} \quad f(x) = 0 \end{array}$$

$$\begin{array}{rccc} \mathcal{N}: & \mathcal{U} \times V & \longrightarrow & V \\ & (f, x) & \mapsto & x - df_x^{-1}(f(x)) \end{array}$$

Itération de Newton

$\mathcal{U}$ — ouvert (d'un sous-ev) de $C^2(B_E(1), F)$

$$\begin{array}{rccl} \mathcal{Z}: & \mathcal{U} & \longrightarrow & V \\ & f & \mapsto & x \quad \text{t.q.} \quad f(x) = 0 \end{array}$$

$$\begin{array}{rccl} \mathcal{N}: & \mathcal{U} \times V & \longrightarrow & V \\ & (f, x) & \mapsto & x - df_x^{-1}(f(x)) \end{array}$$

Différentielles

Itération de Newton

$\mathcal{U}$ — ouvert (d'un sous-ev) de $C^2(B_E(1), F)$

$$\begin{array}{rccc} \mathcal{Z}: & \mathcal{U} & \longrightarrow & V \\ & f & \mapsto & x \quad \text{t.q.} \quad f(x) = 0 \end{array}$$

$$\begin{array}{rccc} \mathcal{N}: & \mathcal{U} \times V & \longrightarrow & V \\ & (f, x) & \mapsto & x - df_x^{-1}(f(x)) \end{array}$$

Différentielles

$$d\mathcal{Z}_f: \qquad \varphi \mapsto -df^{-1}_{\mathcal{Z}(f)}(\varphi(\mathcal{Z}(f)))$$

Itération de Newton

$\mathcal{U}$ — ouvert (d'un sous-ev) de $C^2(B_E(1), F)$

$$\begin{array}{rccl} \mathcal{Z}: & \mathcal{U} & \longrightarrow & V \\ & f & \mapsto & x \quad \text{t.q.} \quad f(x) = 0 \end{array}$$

$$\begin{array}{rccl} \mathcal{N}: & \mathcal{U} \times V & \longrightarrow & V \\ & (f, x) & \mapsto & x - df_x^{-1}(f(x)) \end{array}$$

Différentielles

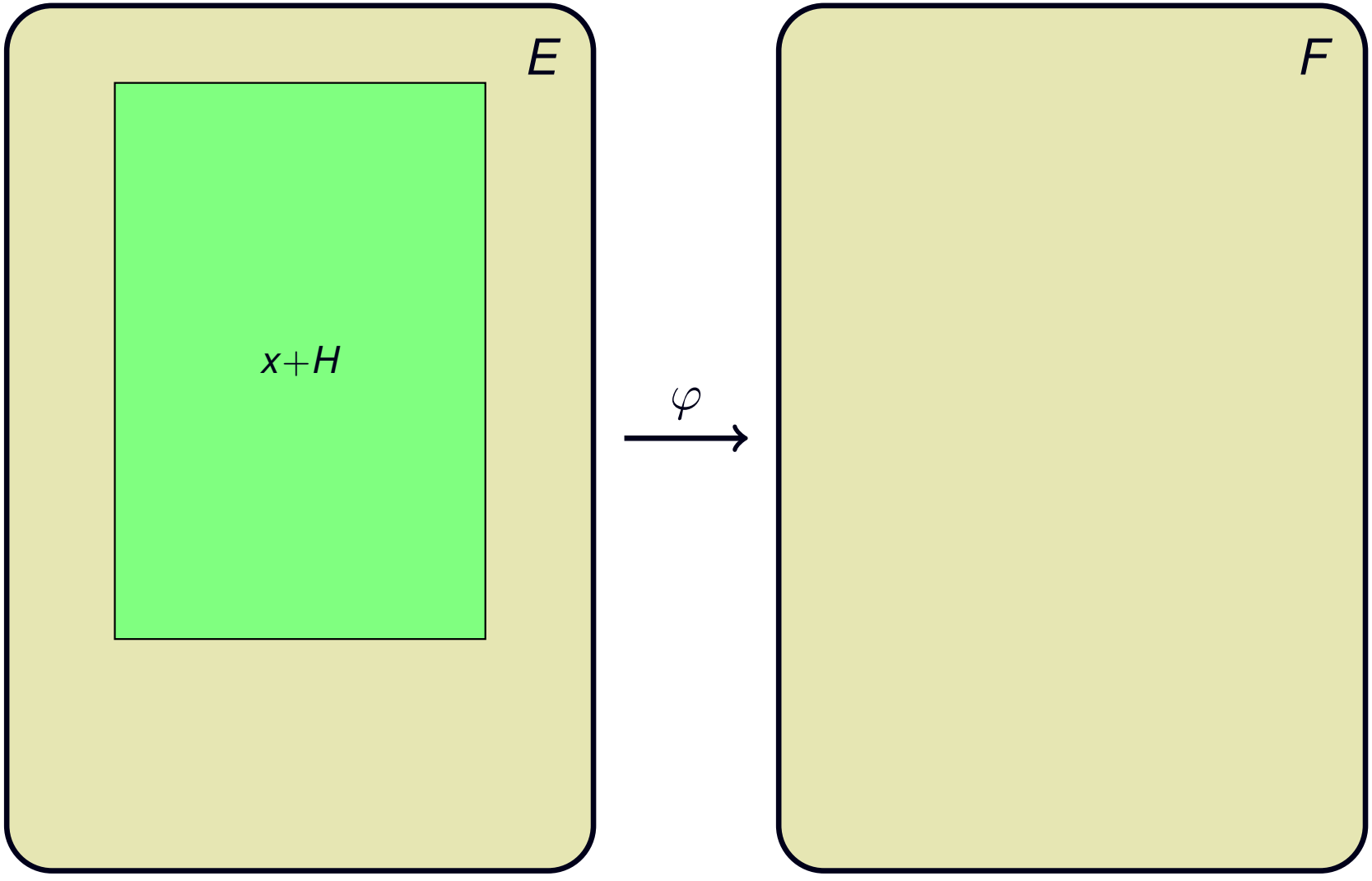
$$d\mathcal{Z}_f : \quad \varphi \quad \mapsto \quad -df^{-1}_{\mathcal{Z}(f)}(\varphi(\mathcal{Z}(f)))$$

$$\begin{array}{rccl} d\mathcal{N}_{(f,x)}: & (\varphi, \xi) & \mapsto & -df_x^{-1}\big(\varphi(x)\big) \\ & & & \quad + df_x^{-1}\big(d^2 f_x(\xi, f(x))\big) \\ & & & \quad + df_x^{-1}\big(d\varphi_x(f(x))\big) \end{array}$$

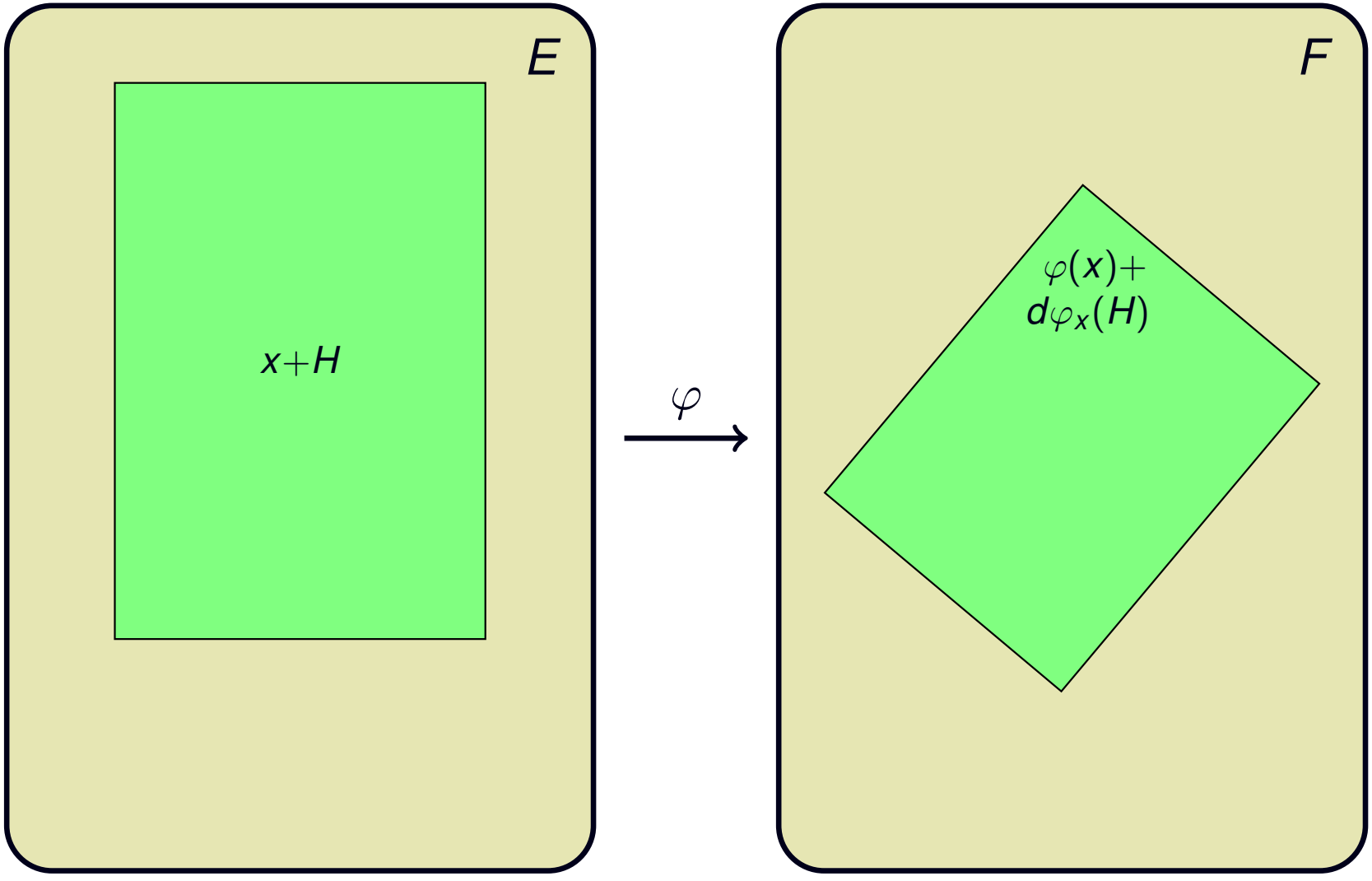
La méthode de la précision adaptative

Contexte de l'arithmétique zélée

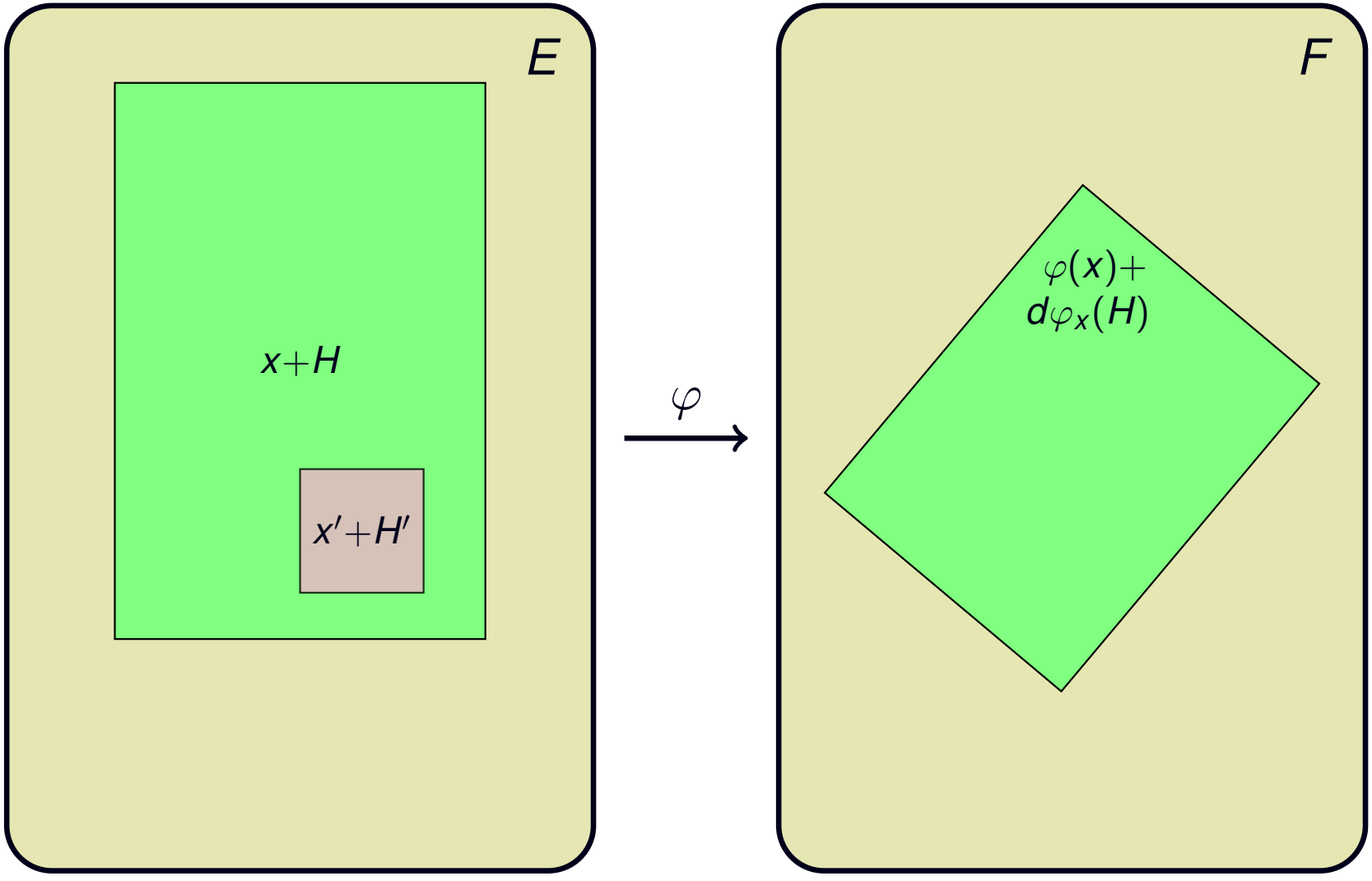
La méthode de la précision adaptative
Contexte de l'arithmétique zélée



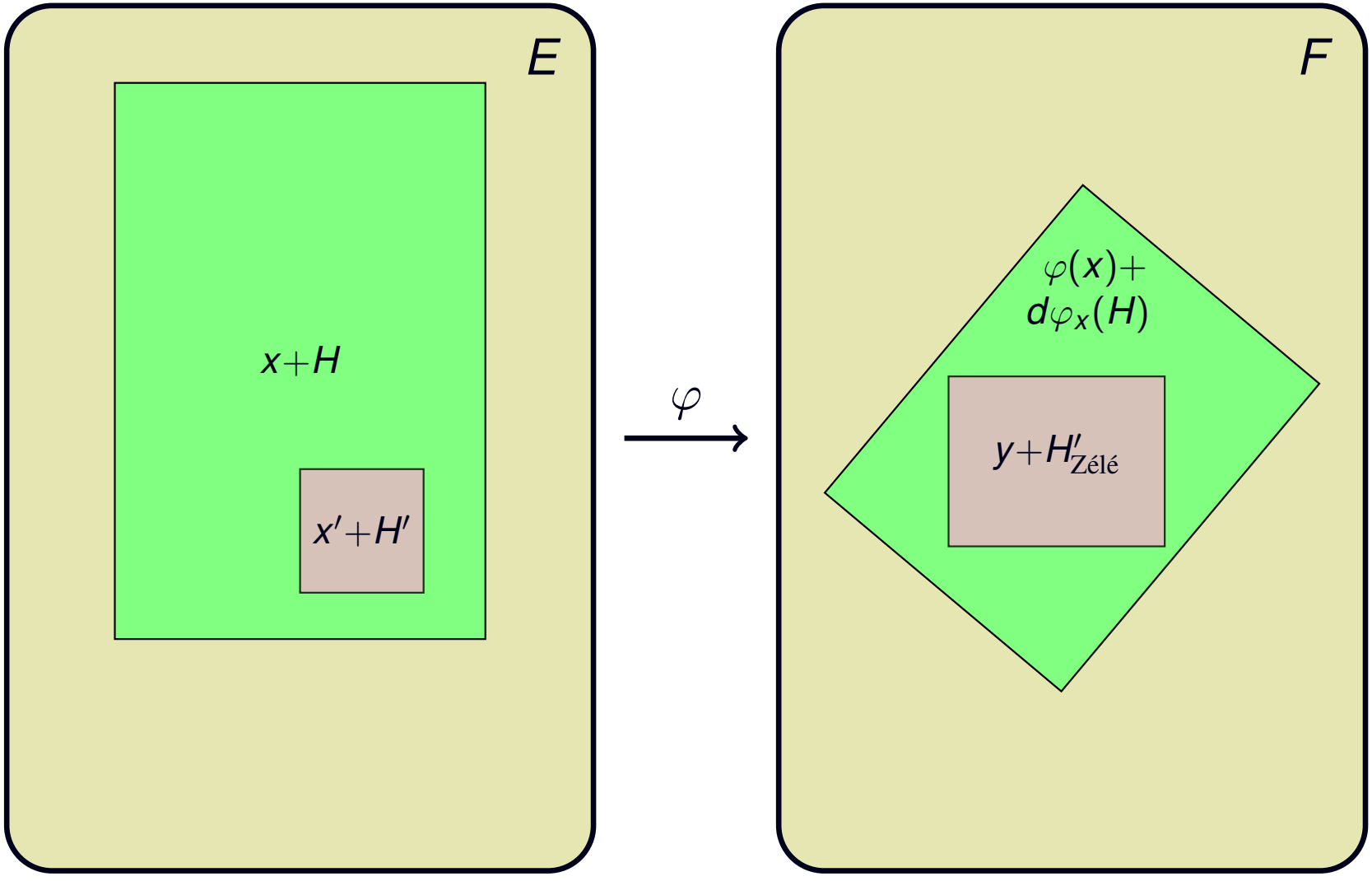
La méthode de la précision adaptative
Contexte de l'arithmétique zélée



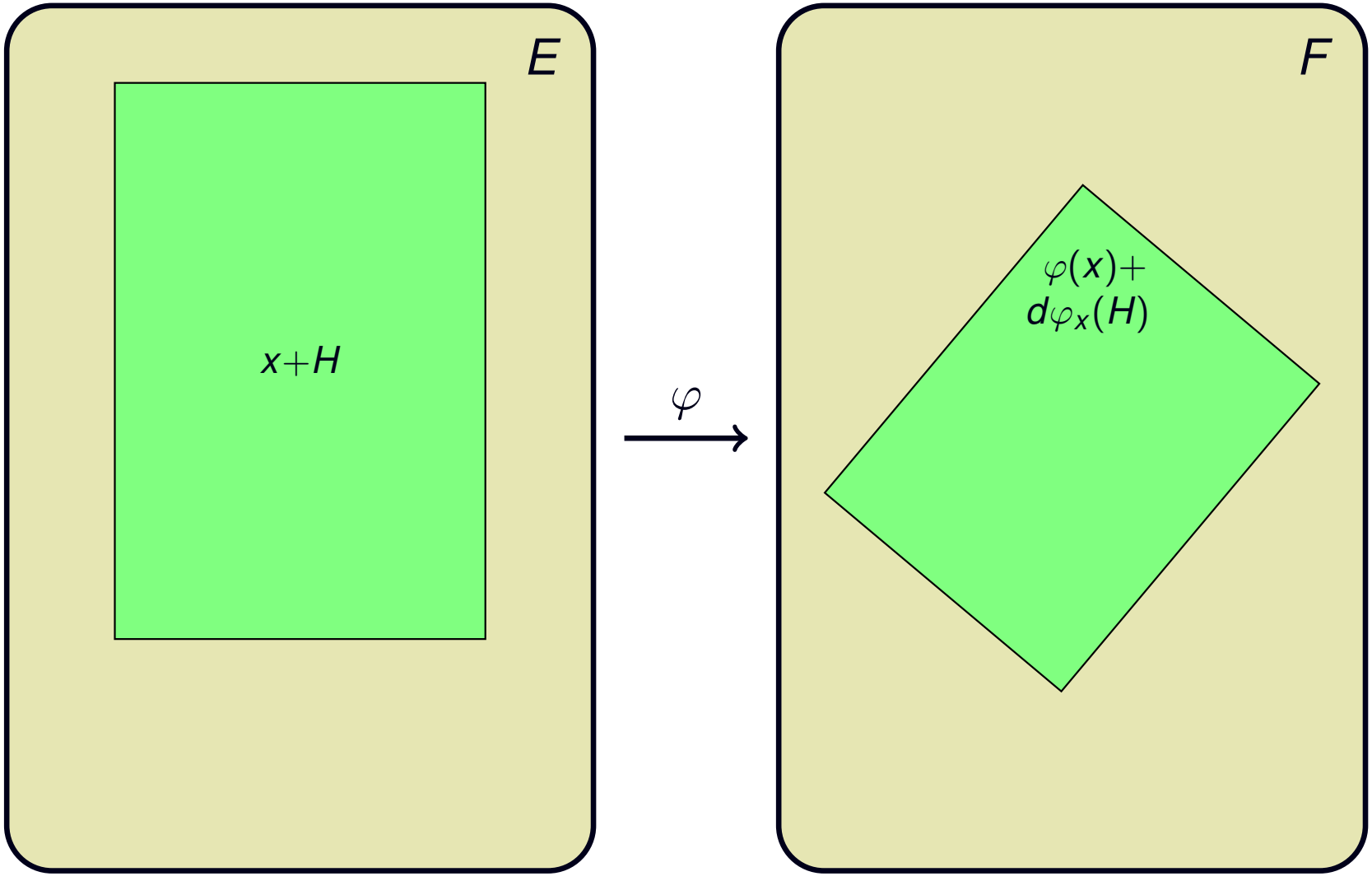
La méthode de la précision adaptative
Contexte de l'arithmétique zélée



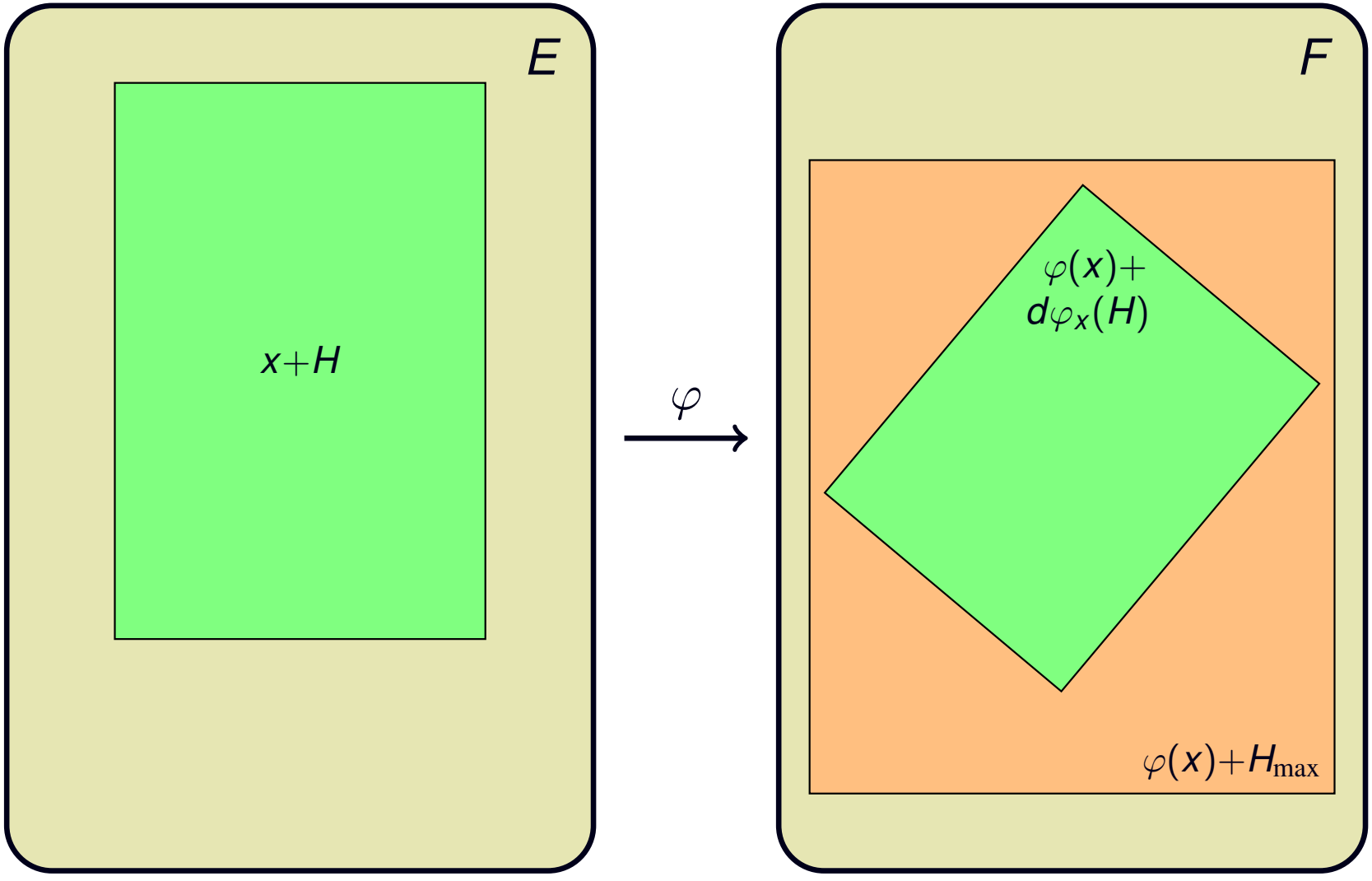
La méthode de la précision adaptative
Contexte de l'arithmétique zélée



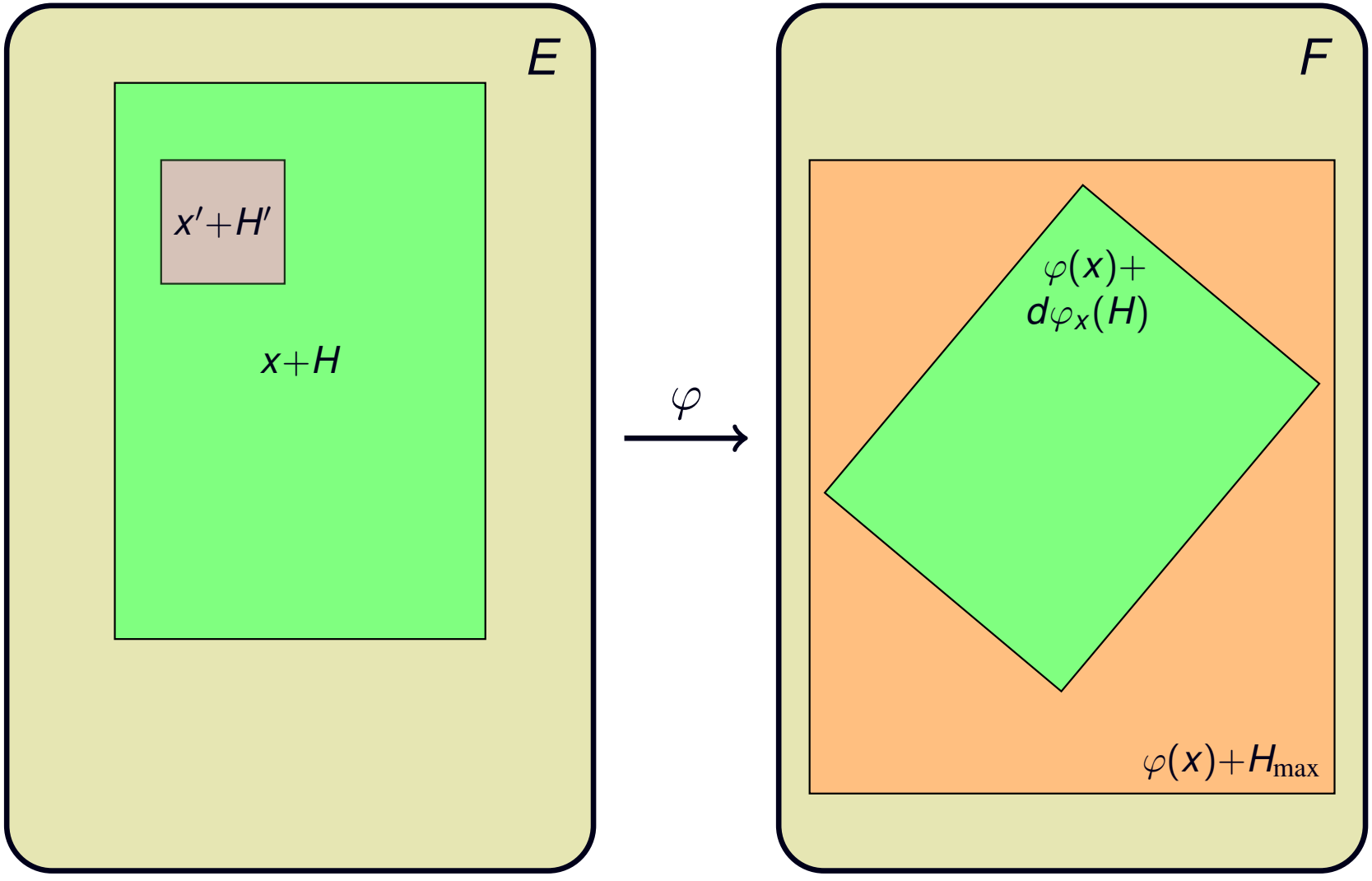
La méthode de la précision adaptative
Contexte de l'arithmétique zélée



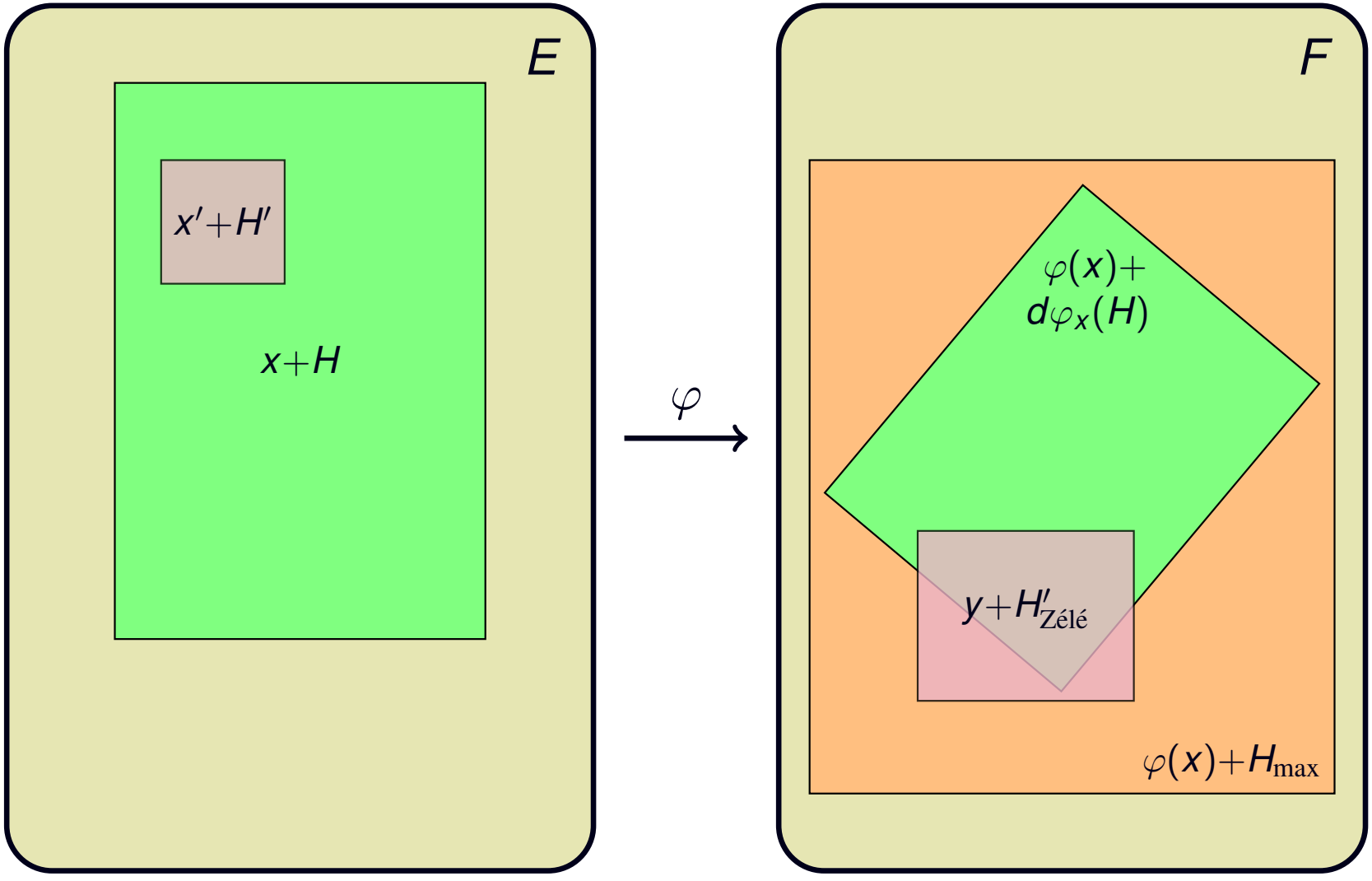
La méthode de la précision adaptative
Contexte de l'arithmétique zélée



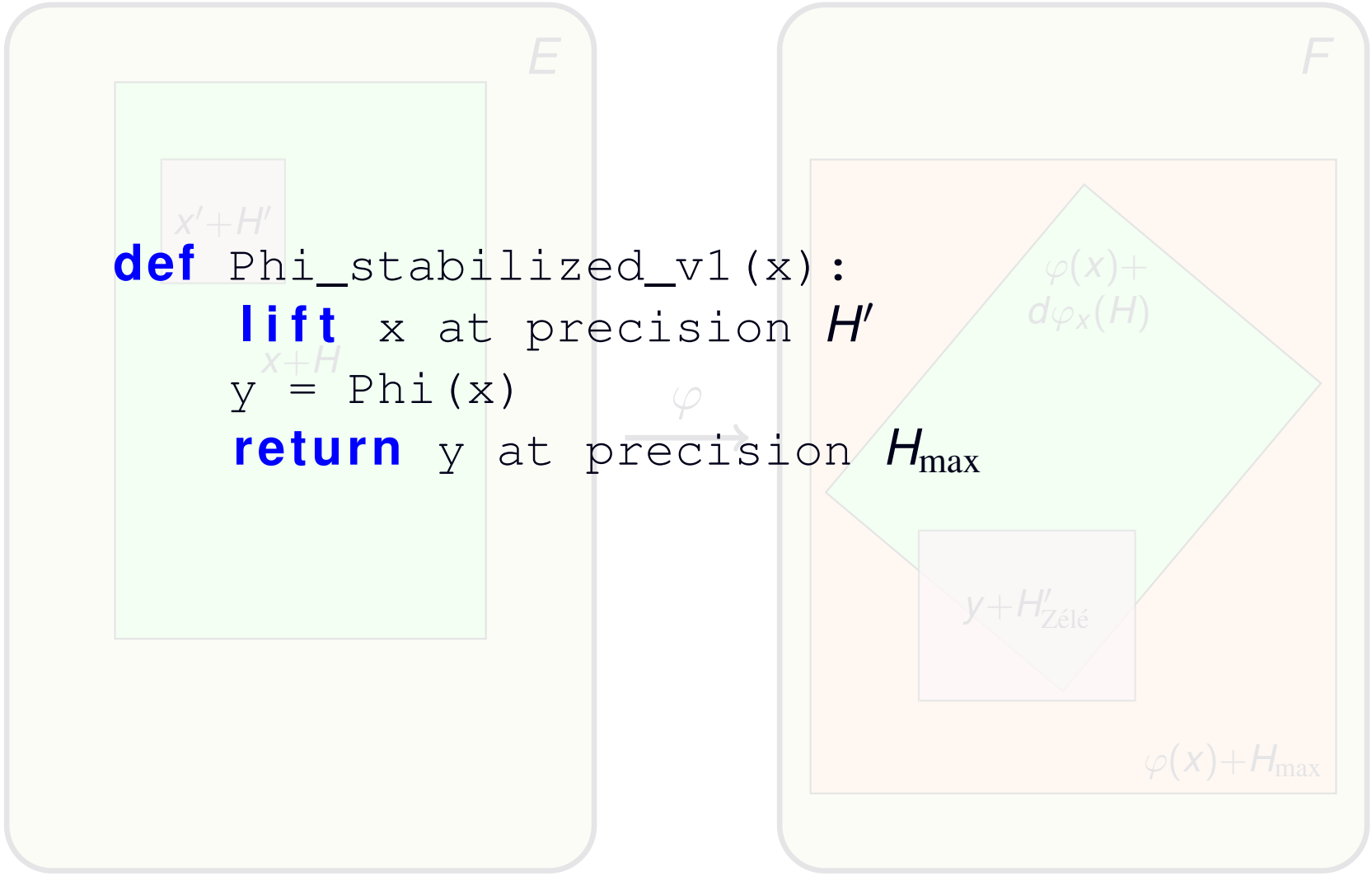
La méthode de la précision adaptative
Contexte de l'arithmétique zélée



La méthode de la précision adaptative
Contexte de l'arithmétique zélée



La méthode de la précision adaptative
Contexte de l'arithmétique zélée



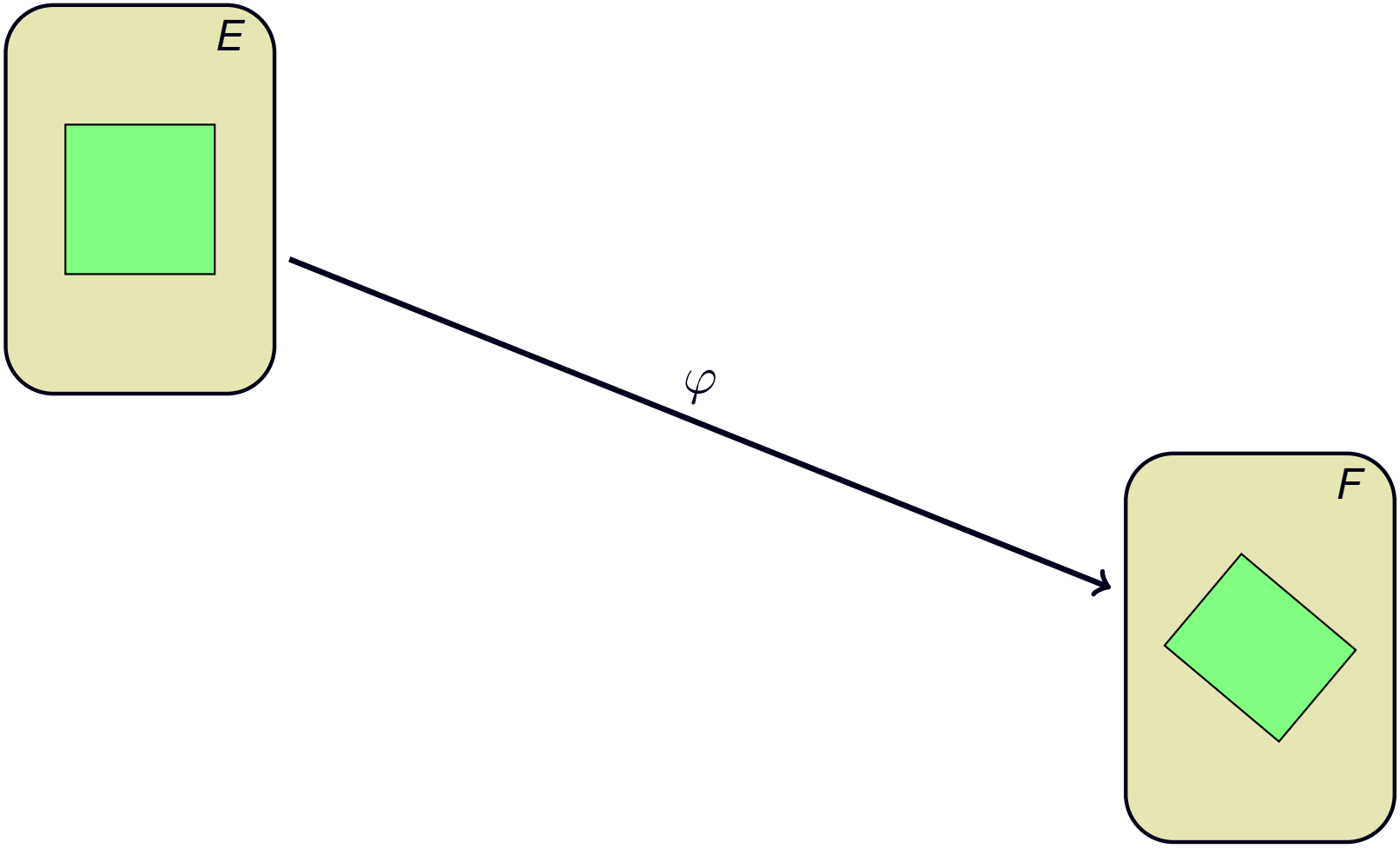

```
def Phi_stabilized_v1(x):
    lift x at precision H'
    y = Phi(x)
    return y at precision H_max
```

La méthode de la précision adaptative

Contexte de l'arithmétique zélée

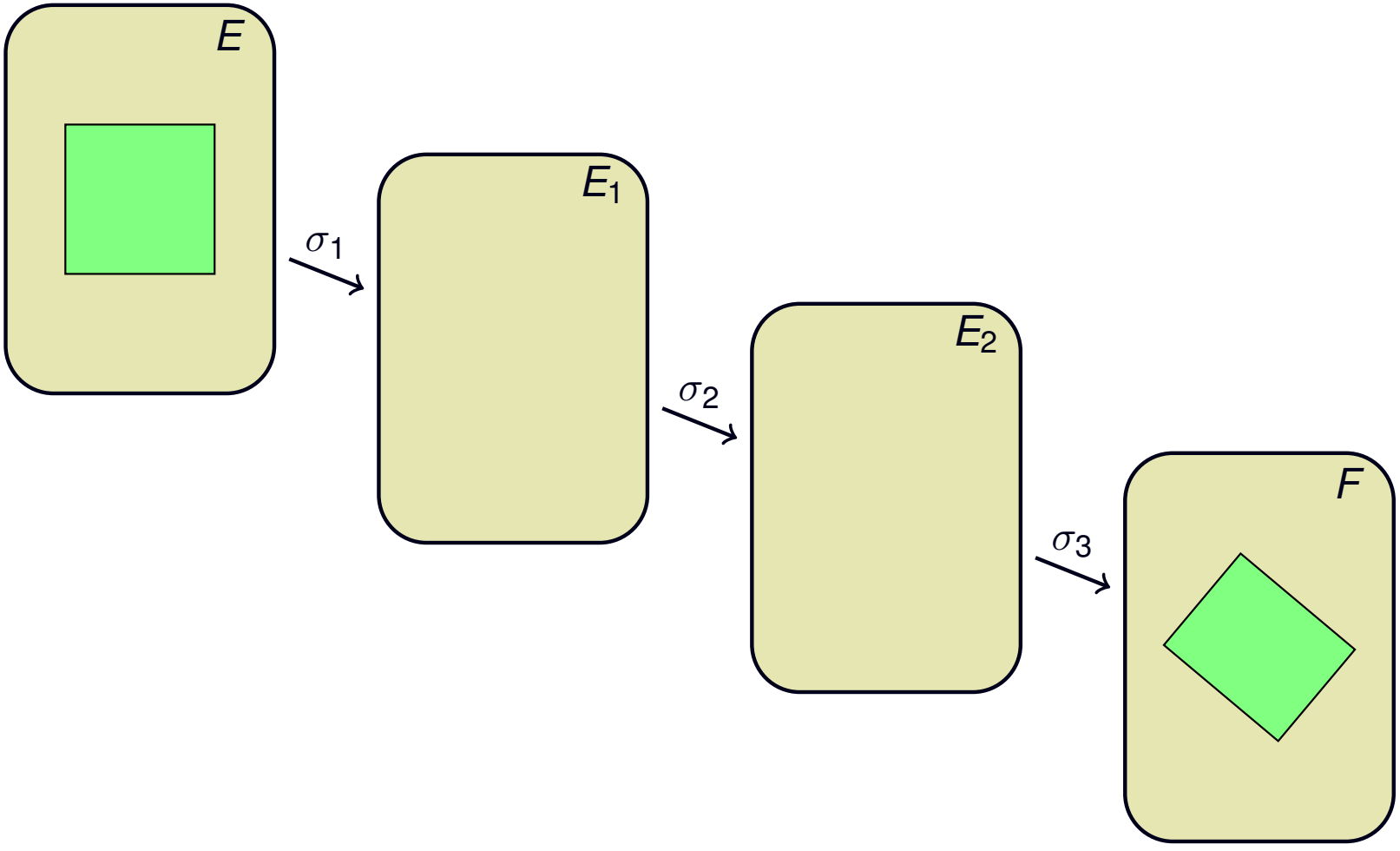
La méthode de la précision adaptative

Contexte de l'arithmétique zélée



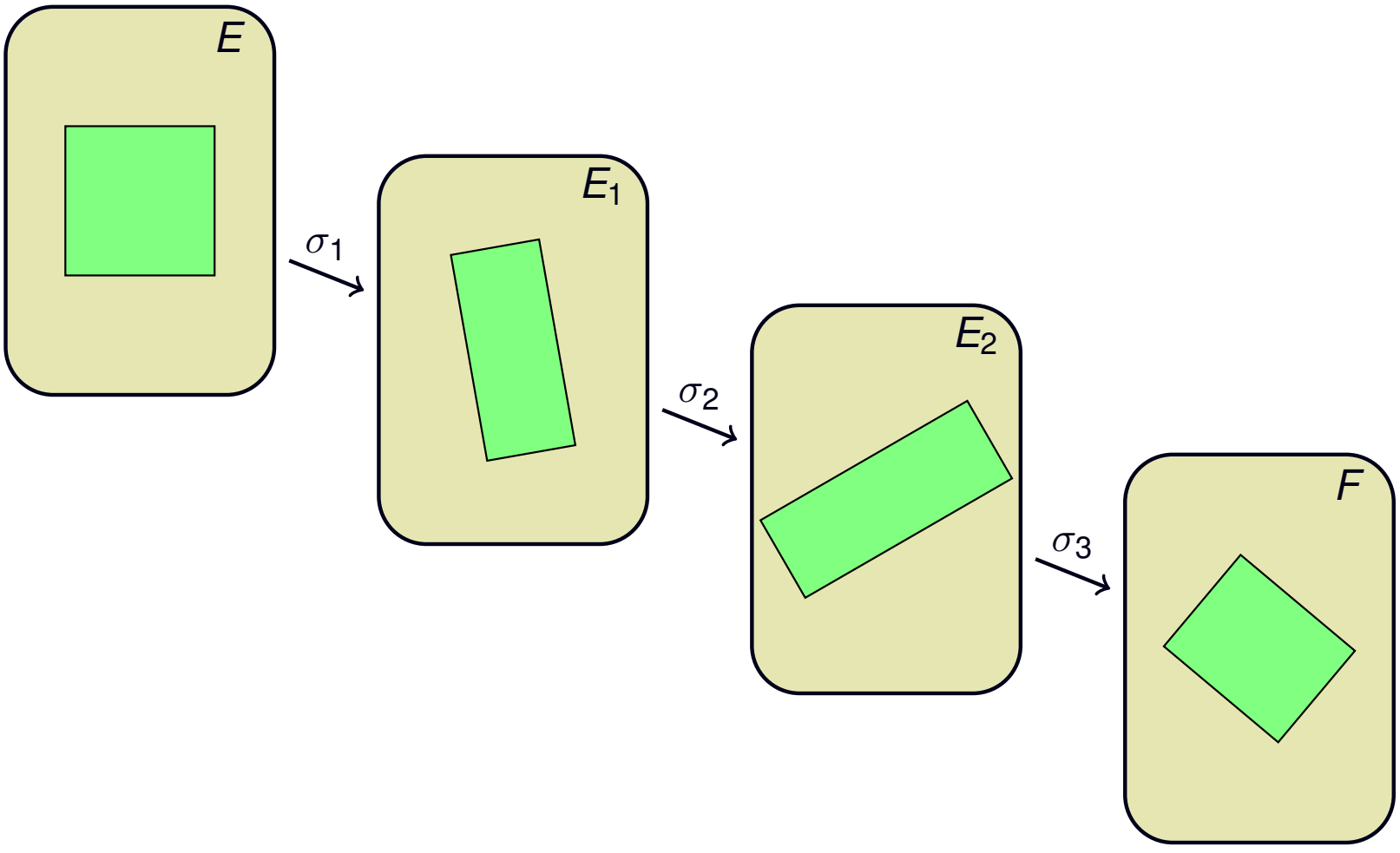
La méthode de la précision adaptative

Contexte de l'arithmétique zélée

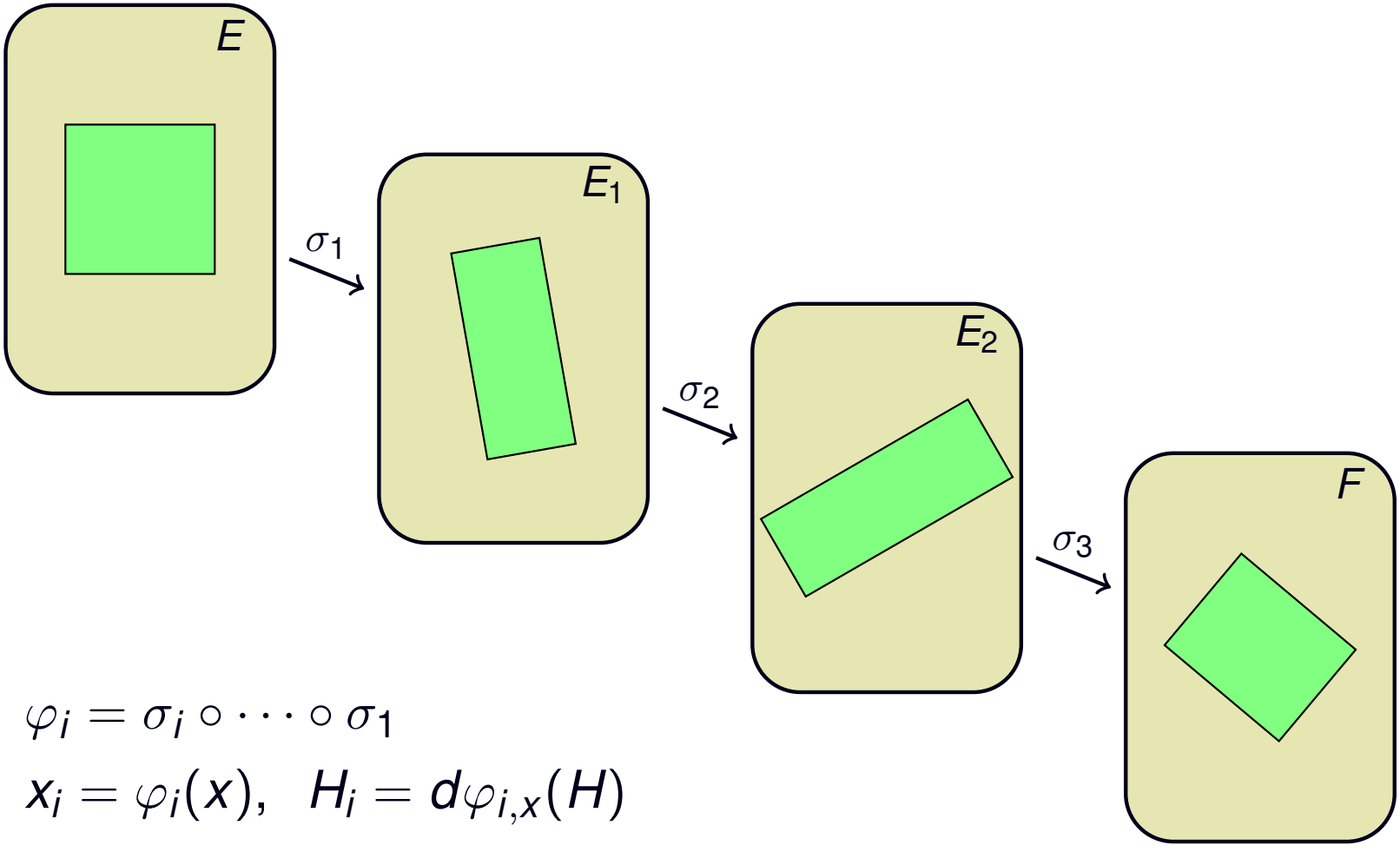


La méthode de la précision adaptative

Contexte de l'arithmétique zélée



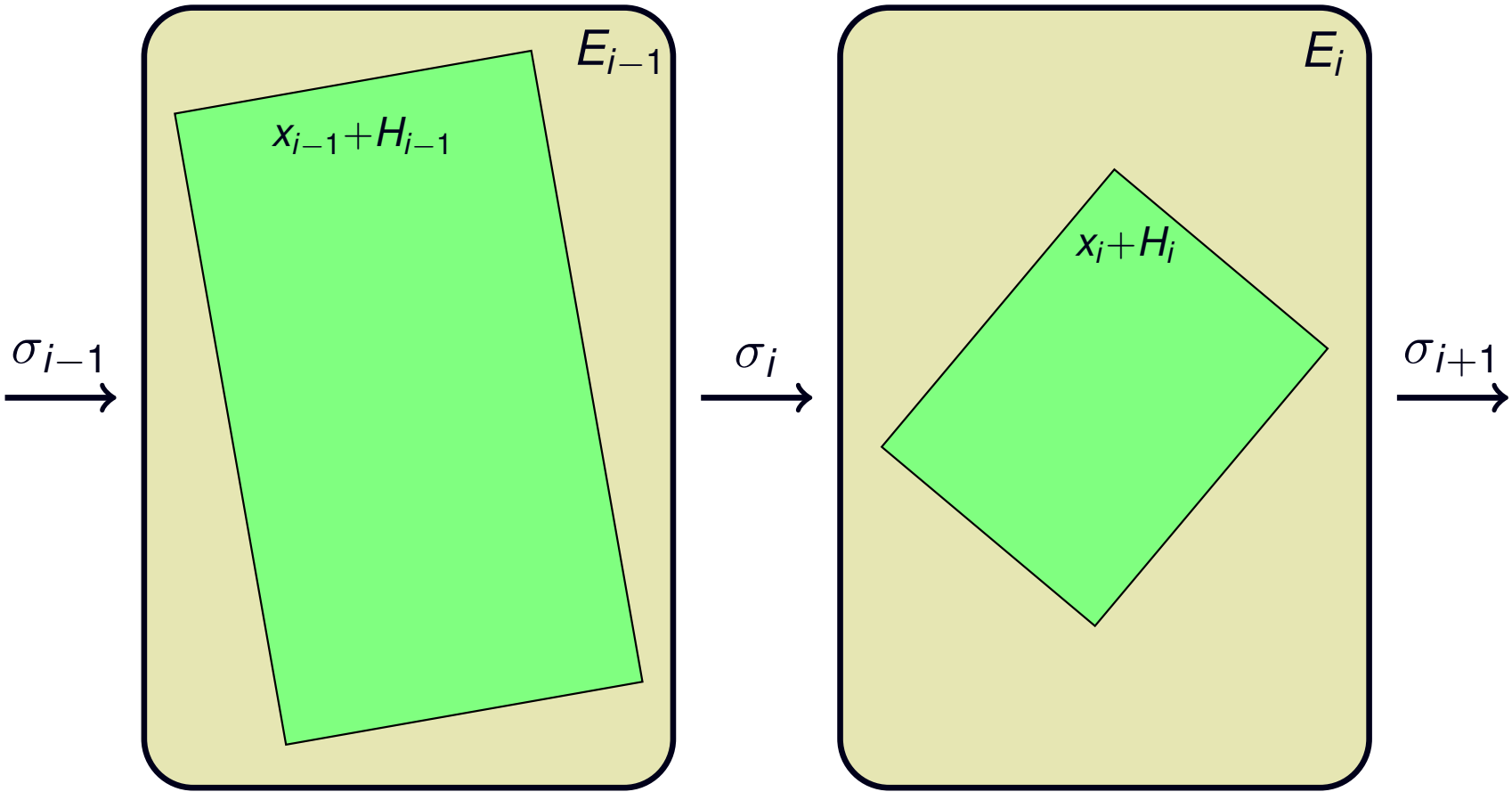
La méthode de la précision adaptative
Contexte de l'arithmétique zélée



$$\varphi_i = \sigma_i \circ \cdots \circ \sigma_1$$

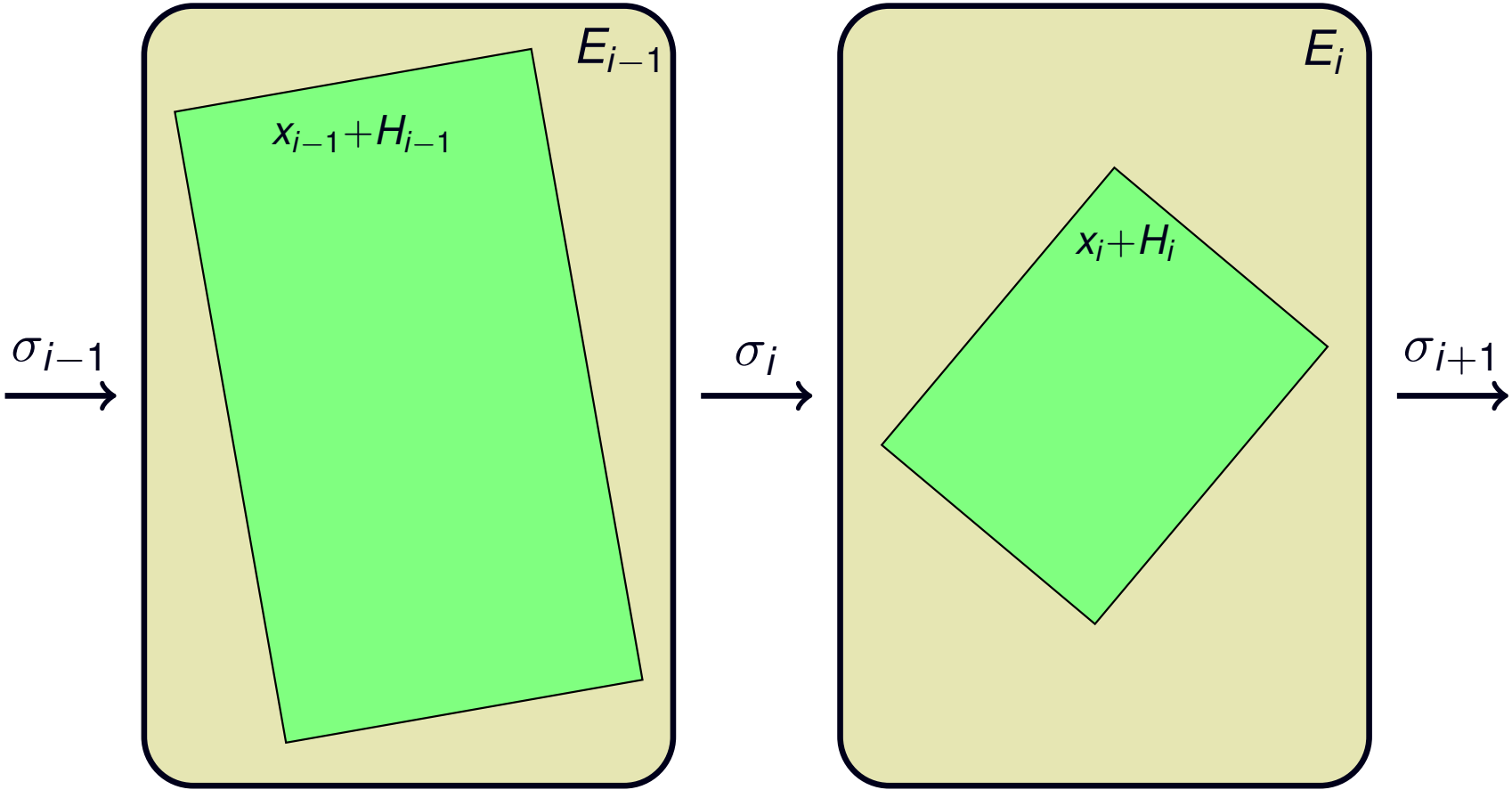
$$x_i = \varphi_i(x), \quad H_i = d\varphi_{i,x}(H)$$

La méthode de la précision adaptative
Contexte de l'arithmétique zélée



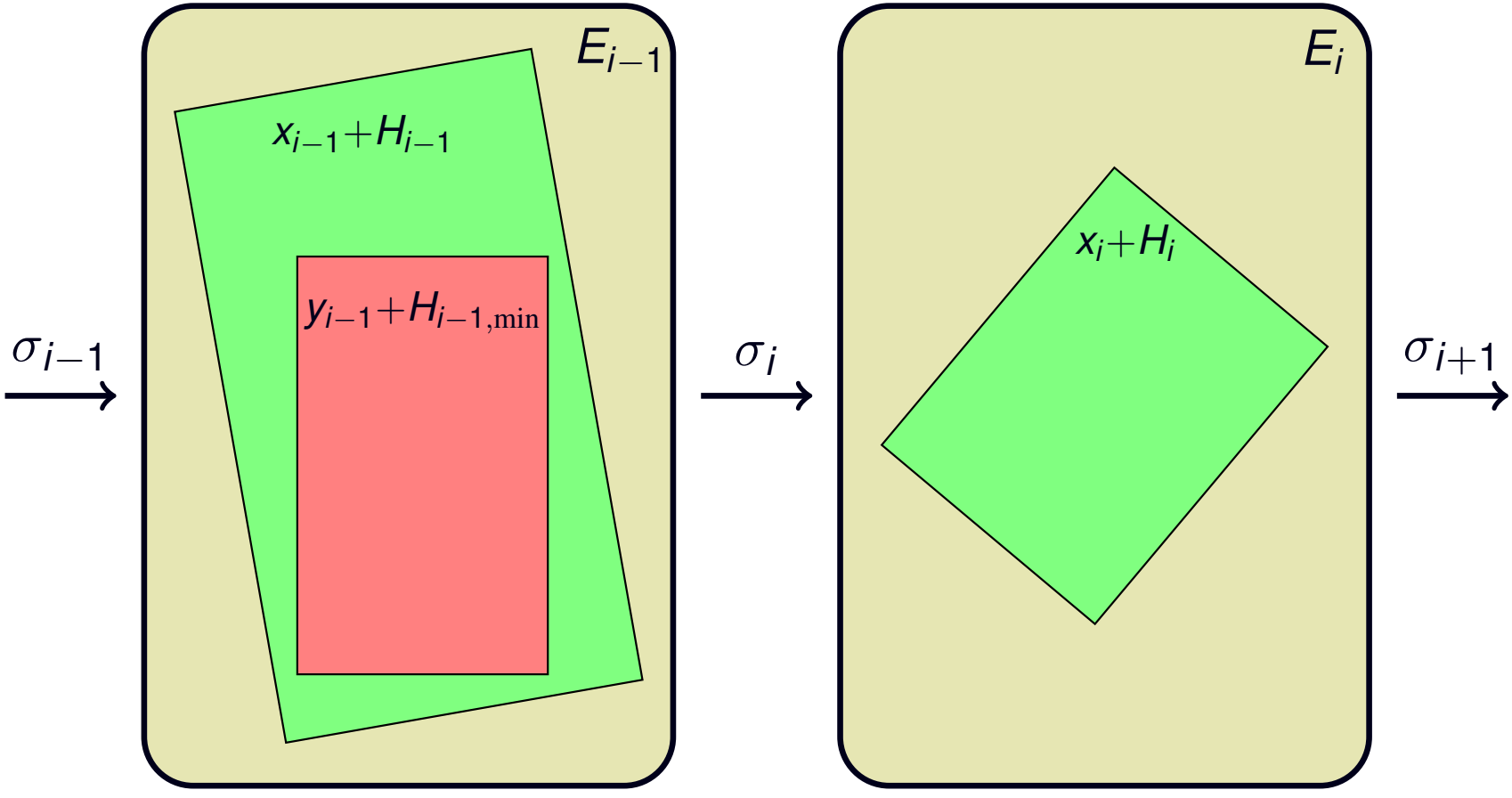
$$\varphi_i = \sigma_i \circ \cdots \circ \sigma_1, \quad x_i = \varphi_i(x), \quad H_i = d\varphi_{i,x}(H)$$

La méthode de la précision adaptative
Contexte de l'arithmétique zélée



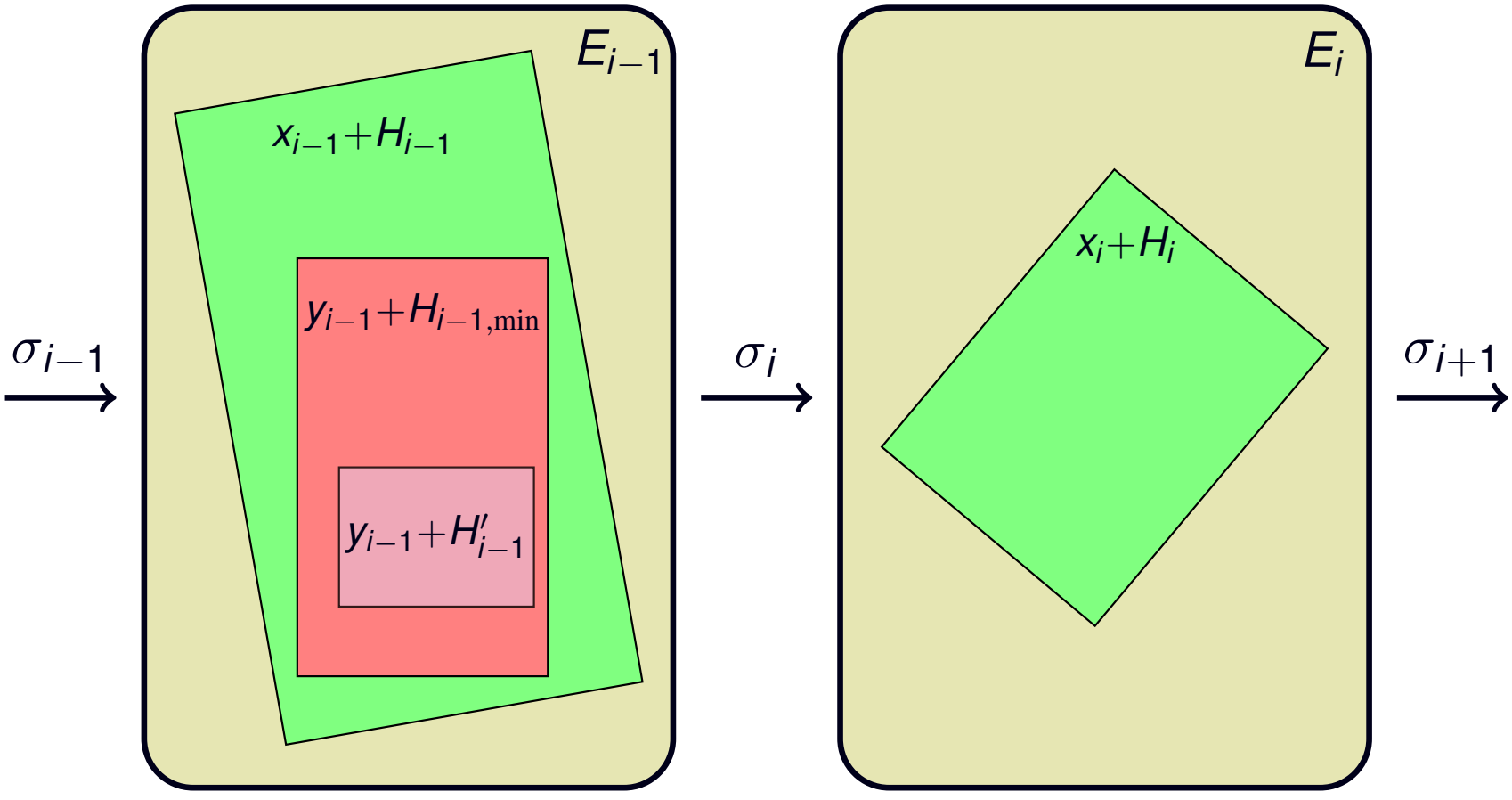
$\varphi_i = \sigma_i \circ \cdots \circ \sigma_1, \quad x_i = \varphi_i(x), \quad H_i = d\varphi_{i,x}(H) \qquad H_{i,\min} \subset H_i$

La méthode de la précision adaptative
Contexte de l'arithmétique zélée



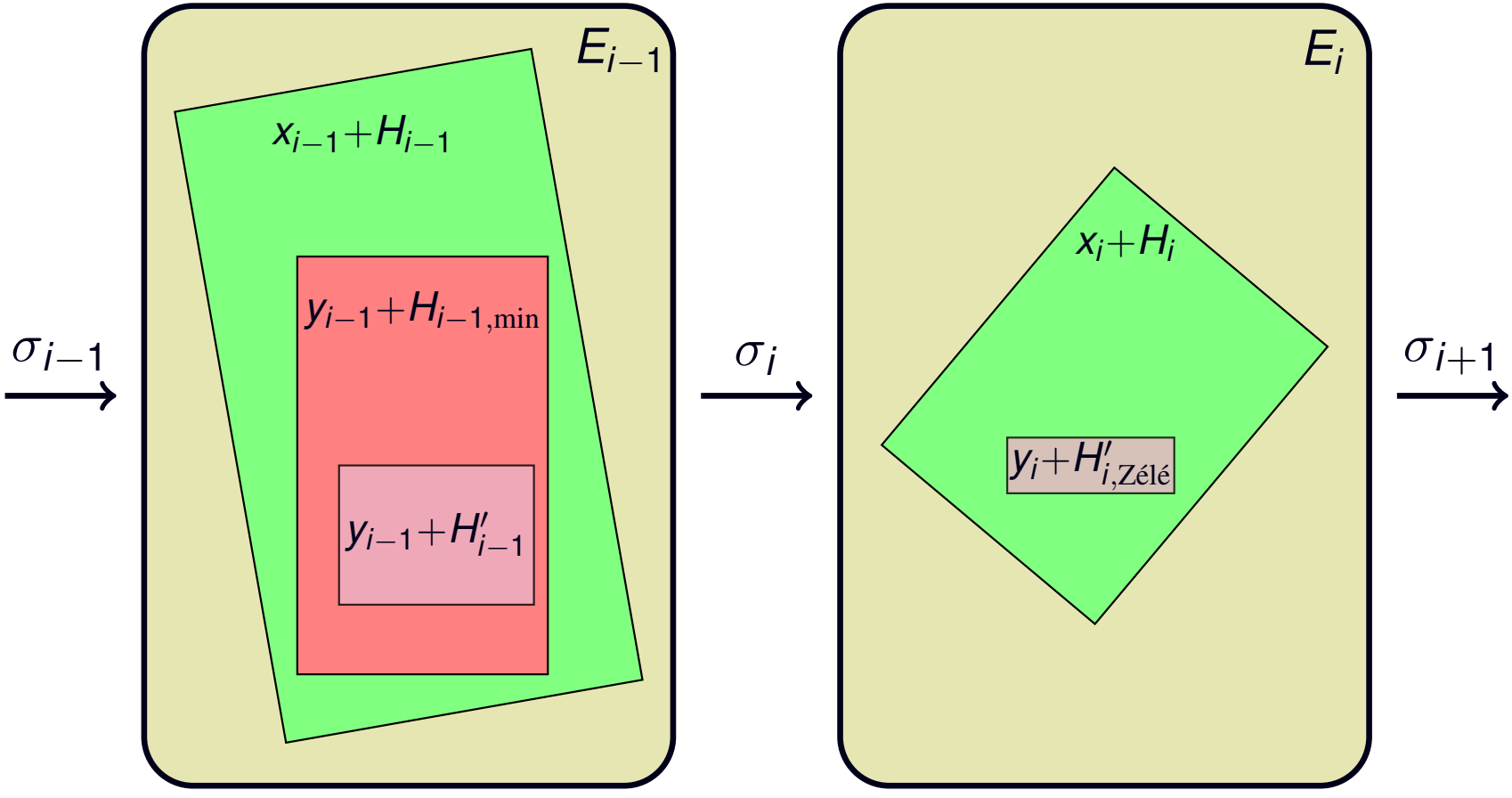
$$\varphi_i = \sigma_i \circ \cdots \circ \sigma_1, \quad x_i = \varphi_i(x), \quad H_i = d\varphi_{i,x}(H) \qquad H_{i,\min} \subset H_i$$

La méthode de la précision adaptative
Contexte de l'arithmétique zélée



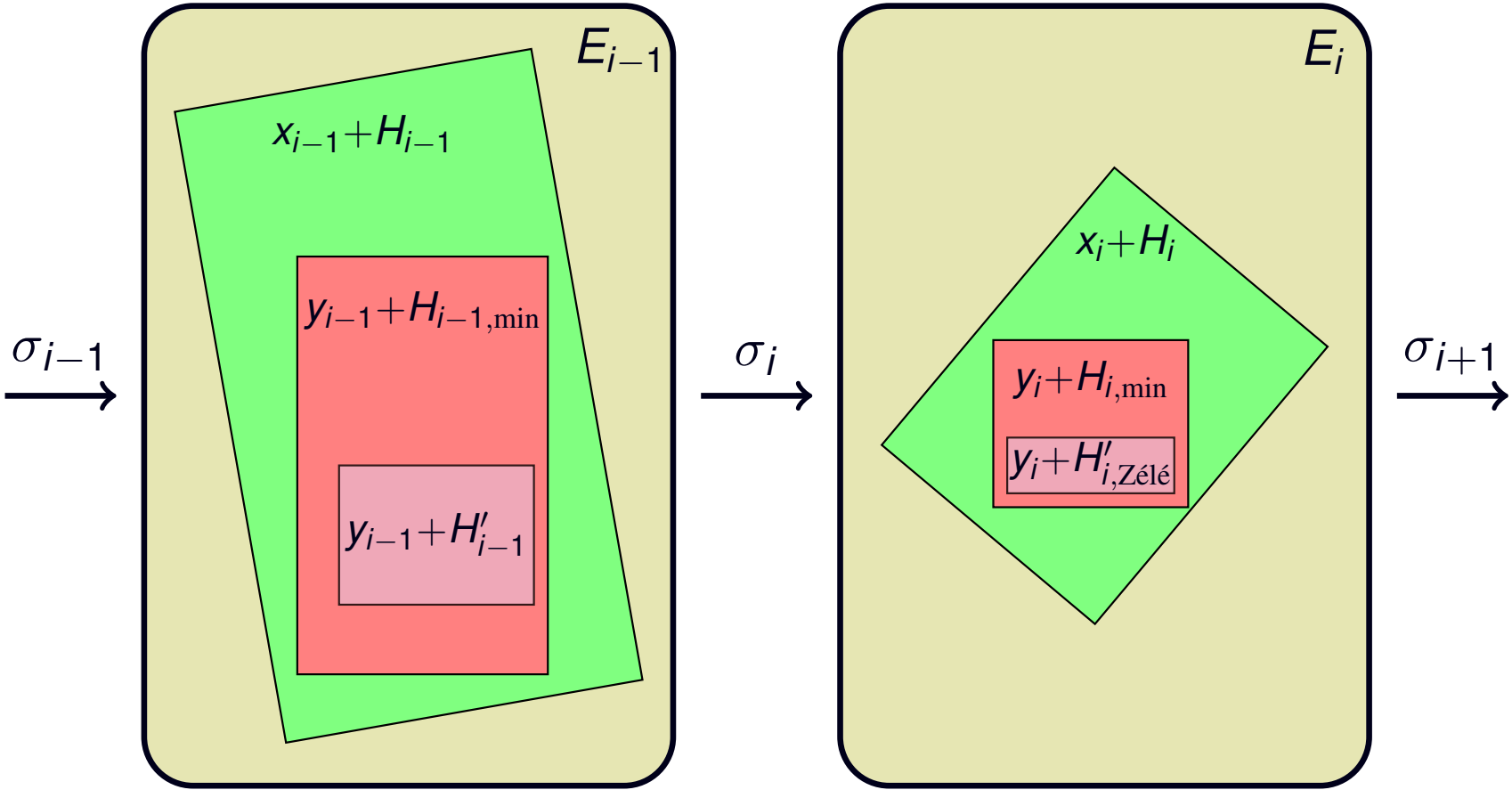
$$\varphi_i = \sigma_i \circ \cdots \circ \sigma_1, \quad x_i = \varphi_i(x), \quad H_i = d\varphi_{i,x}(H) \qquad H_{i,\min} \subset H_i$$

La méthode de la précision adaptative
Contexte de l'arithmétique zélée



$$\varphi_i = \sigma_i \circ \cdots \circ \sigma_1, \quad x_i = \varphi_i(x), \quad H_i = d\varphi_{i,x}(H) \qquad H_{i,\min} \subset H_i$$

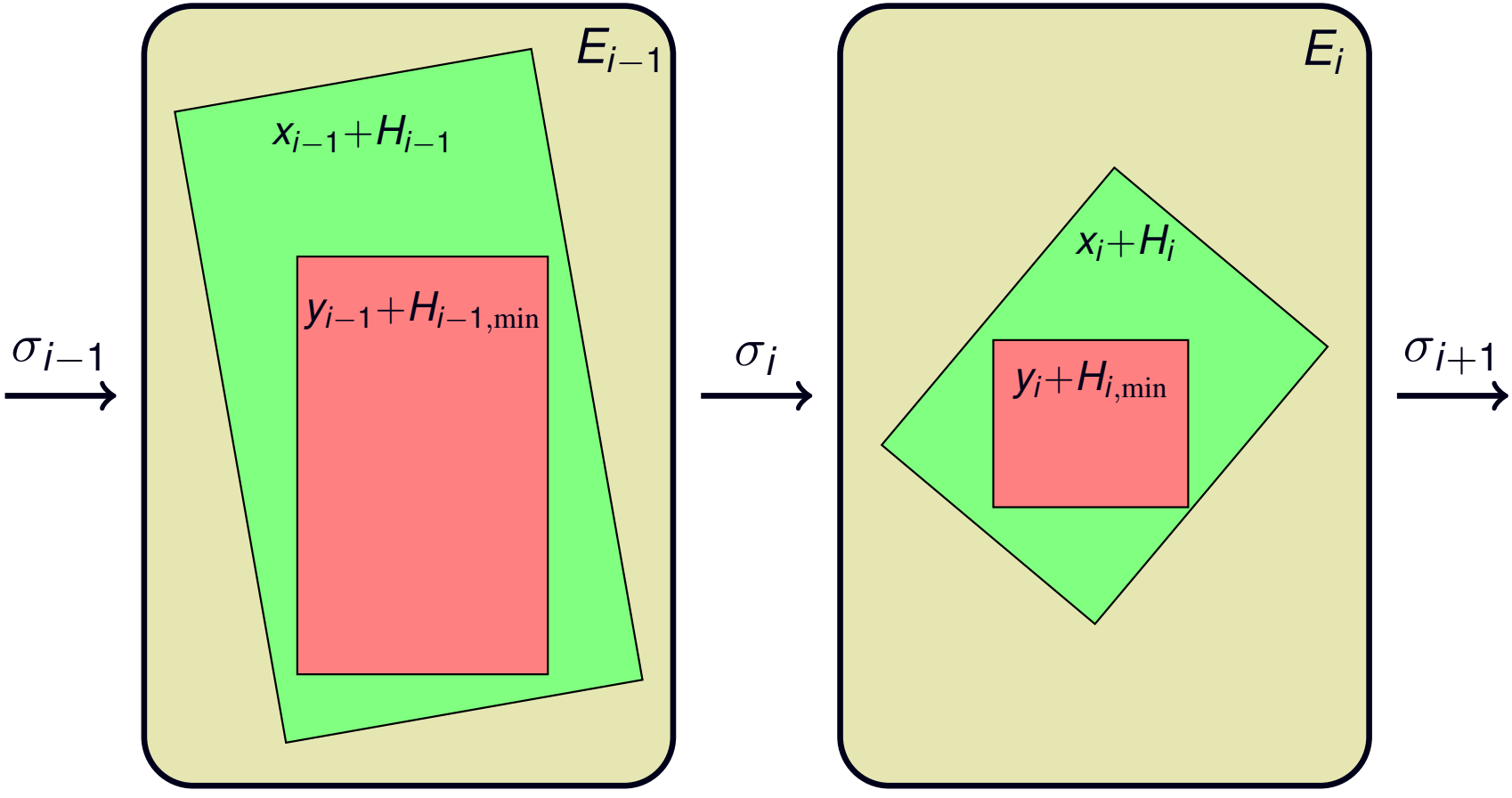
La méthode de la précision adaptative
Contexte de l'arithmétique zélée



$$\varphi_i = \sigma_i \circ \cdots \circ \sigma_1, \quad x_i = \varphi_i(x), \quad H_i = d\varphi_{i,x}(H) \qquad H_{i,\min} \subset H_i$$

La méthode de la précision adaptative

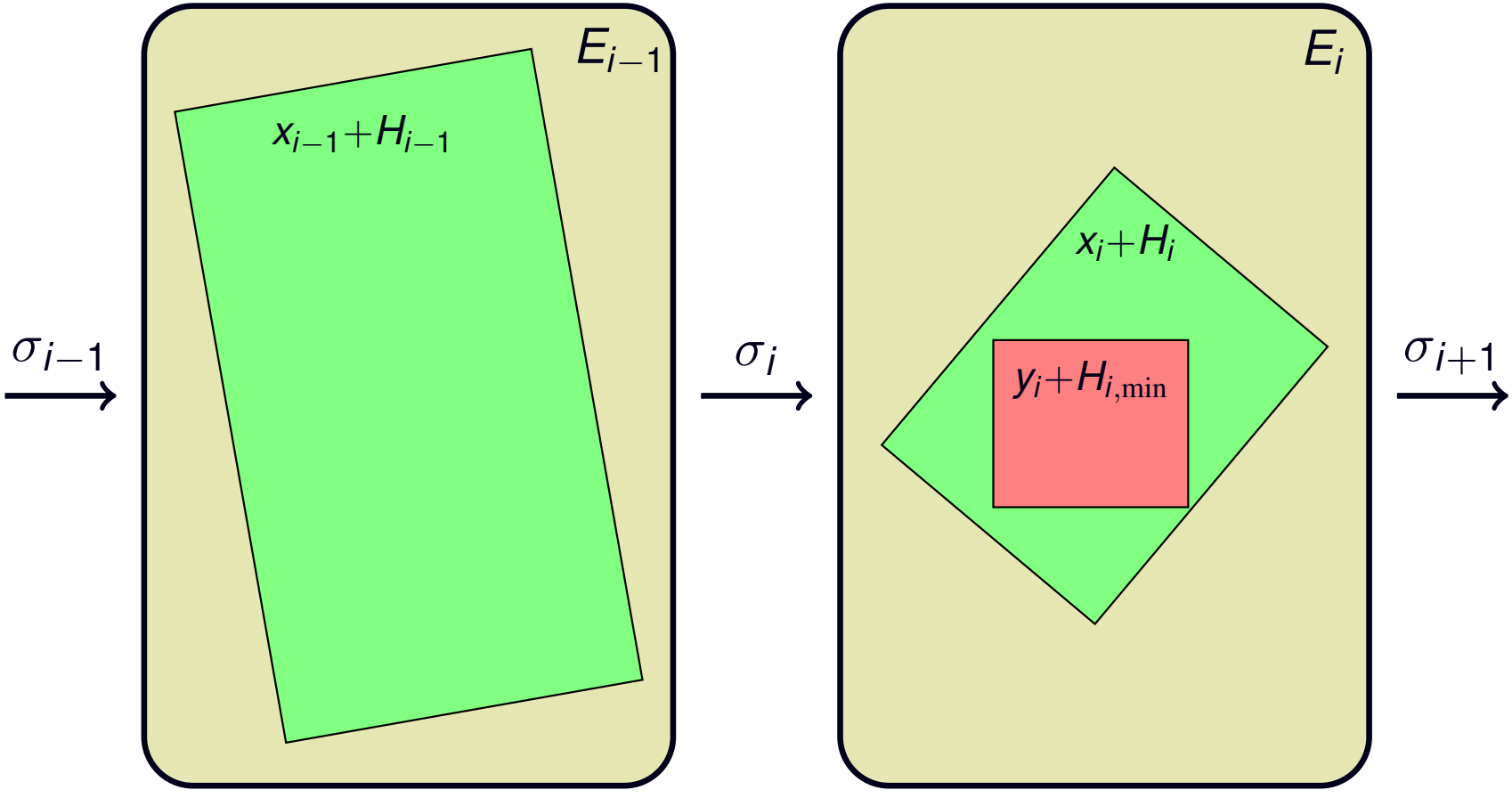
Contexte de l'arithmétique zélée



$$\varphi_i = \sigma_i \circ \cdots \circ \sigma_1, \quad x_i = \varphi_i(x), \quad H_i = d\varphi_{i,x}(H) \qquad H_{i,\min} \subset H_i$$

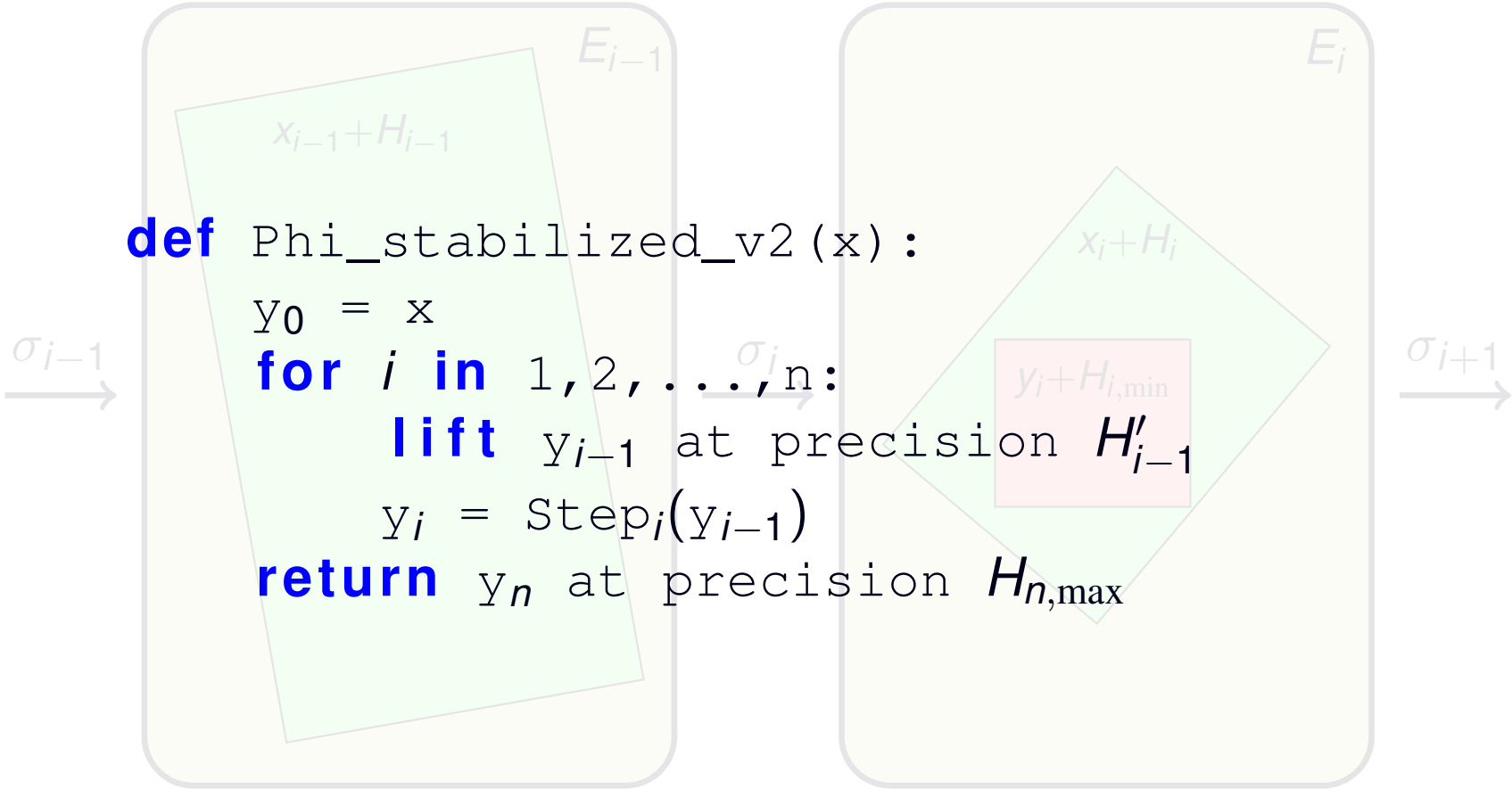
La méthode de la précision adaptative

Contexte de l'arithmétique zélée



$$\varphi_i = \sigma_i \circ \cdots \circ \sigma_1, \quad x_i = \varphi_i(x), \quad H_i = d\varphi_{i,x}(H) \qquad H_{i,\min} \subset H_i$$

La méthode de la précision adaptative
Contexte de l'arithmétique zélée




```
def Phi_stabilized_v2(x):
    y0 = x
    for i in 1,2,...,n:
        lift y_{i-1} at precision H'_{i-1}
        y_i = Step_i(y_{i-1})
    return y_n at precision H_{n,max}
```

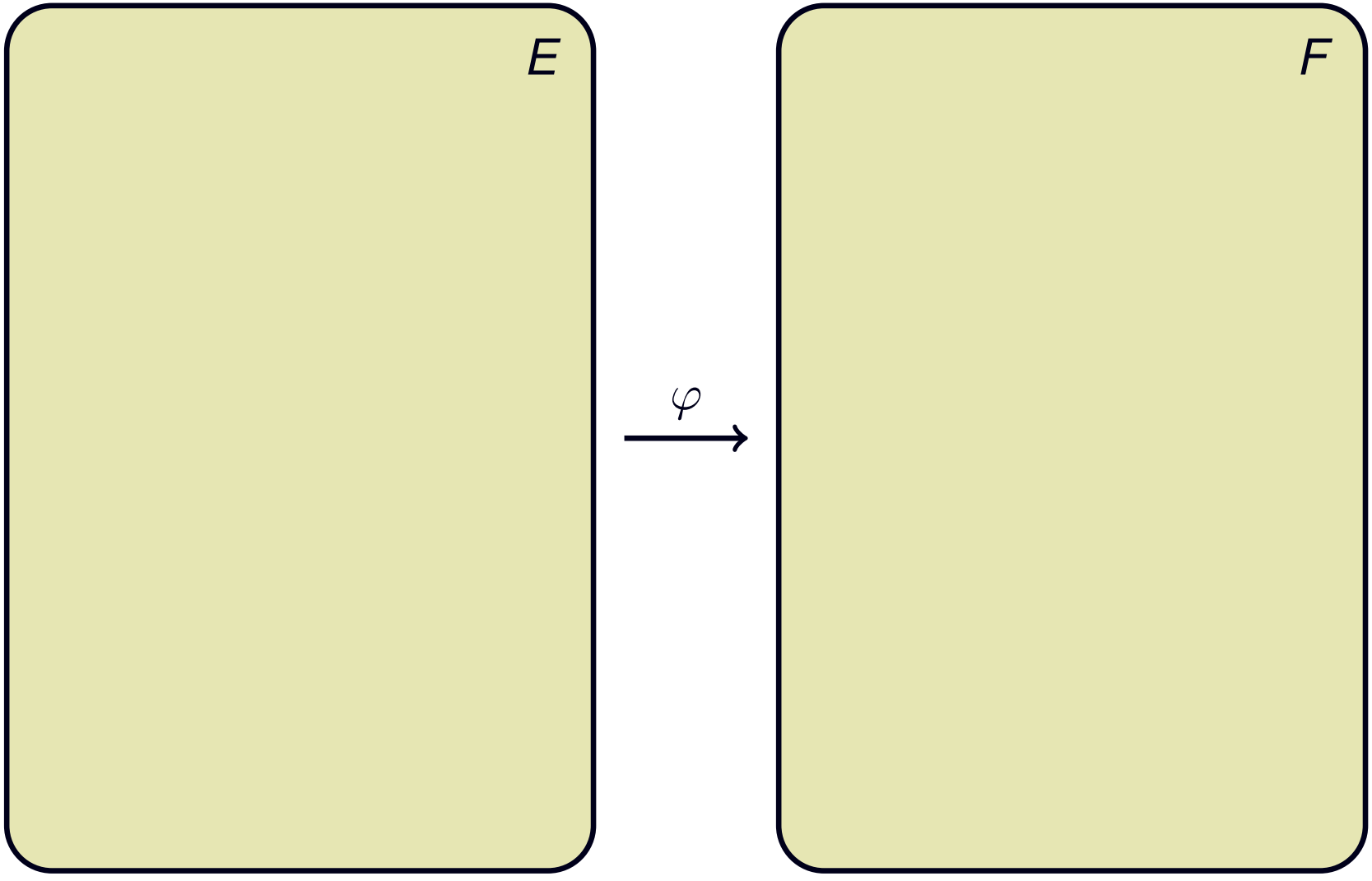
$\varphi_i = \sigma_i \circ \cdots \circ \sigma_1, \quad x_i = \varphi_i(x), \quad H_i = d\varphi_{i,x}(H) \qquad H_{i,\min} \subset H_i$

La méthode de la précision adaptative

Contexte de l'arithmétique paresseuse

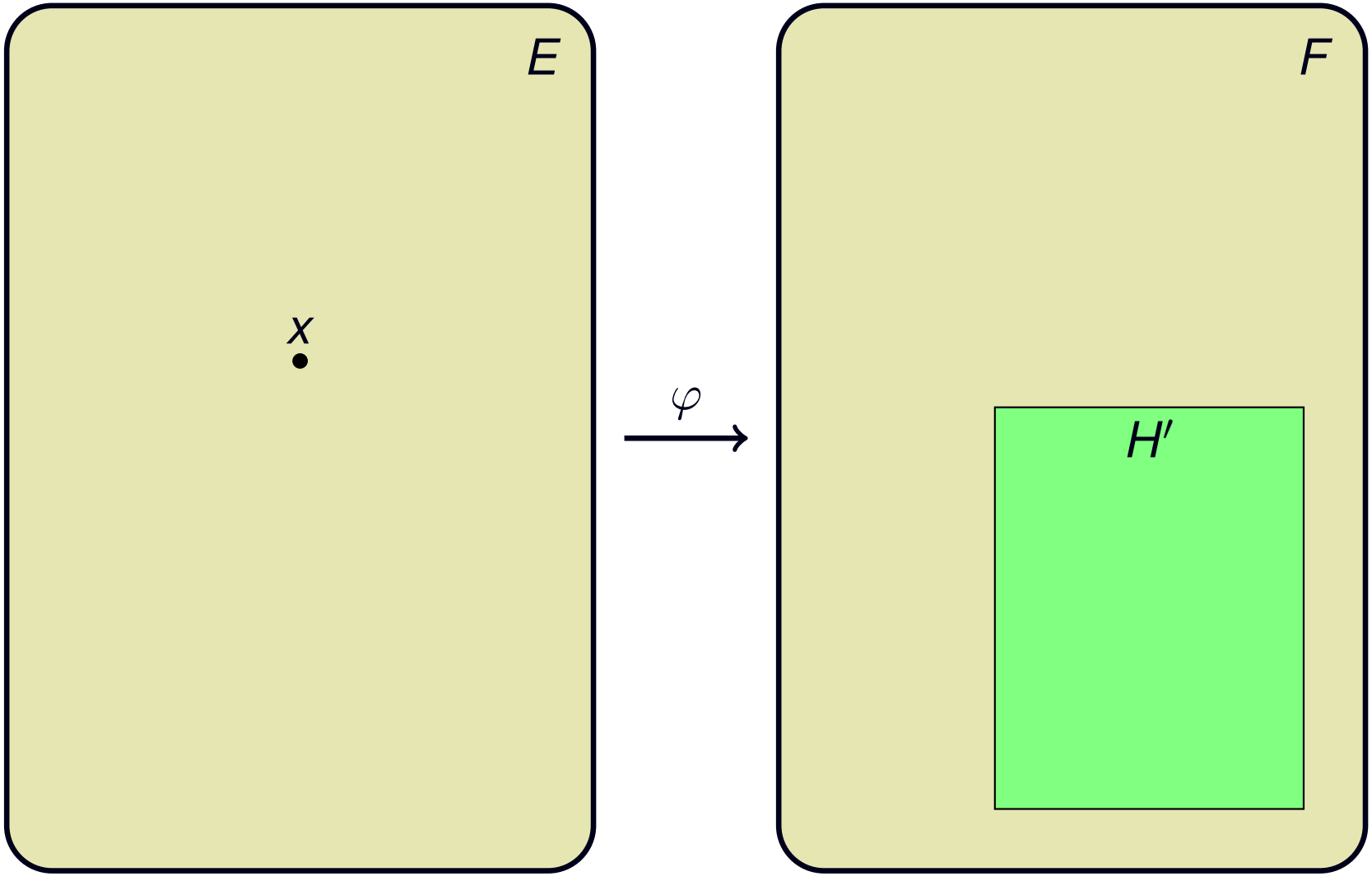
La méthode de la précision adaptative

Contexte de l'arithmétique paresseuse

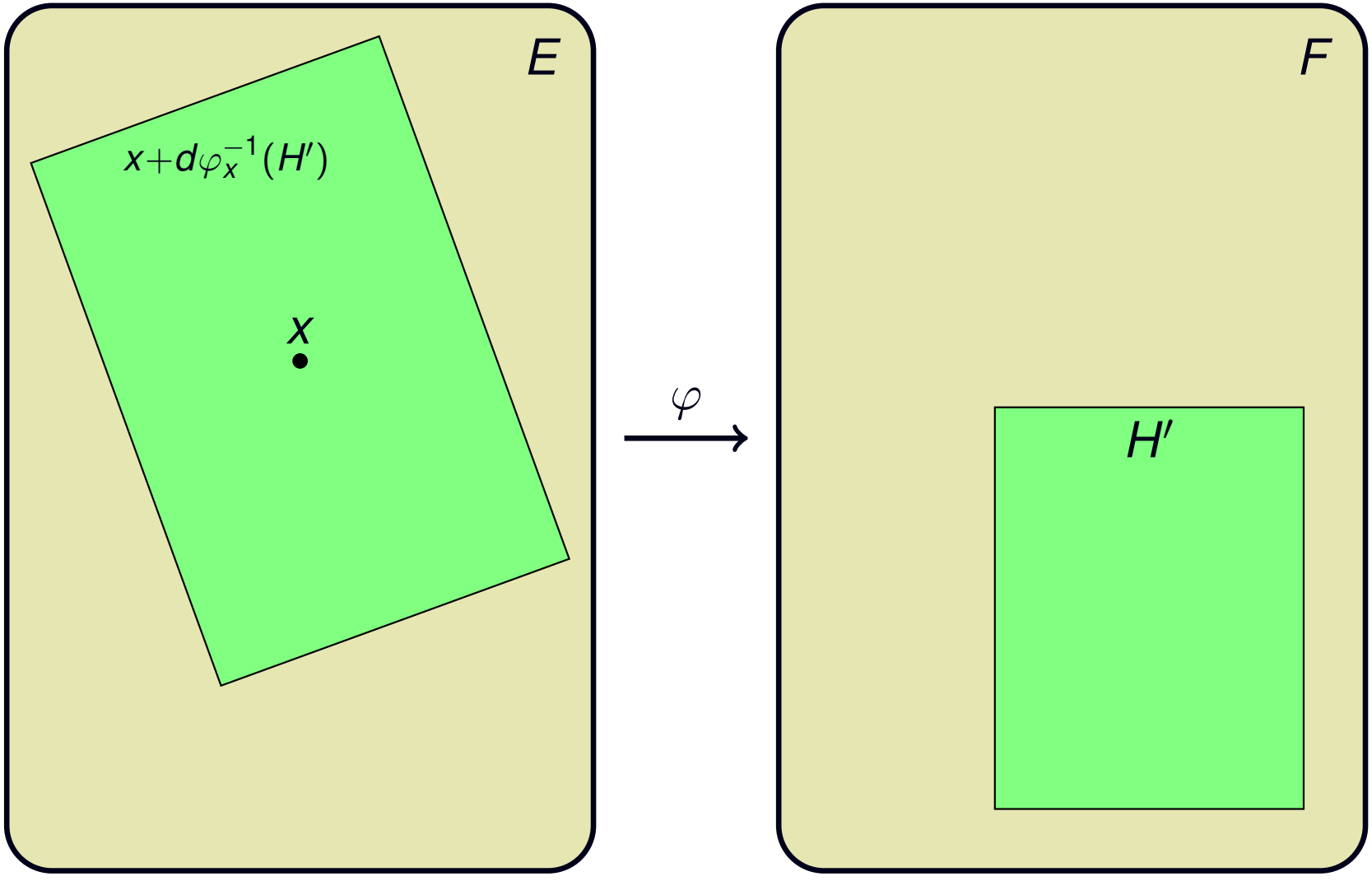


La méthode de la précision adaptative

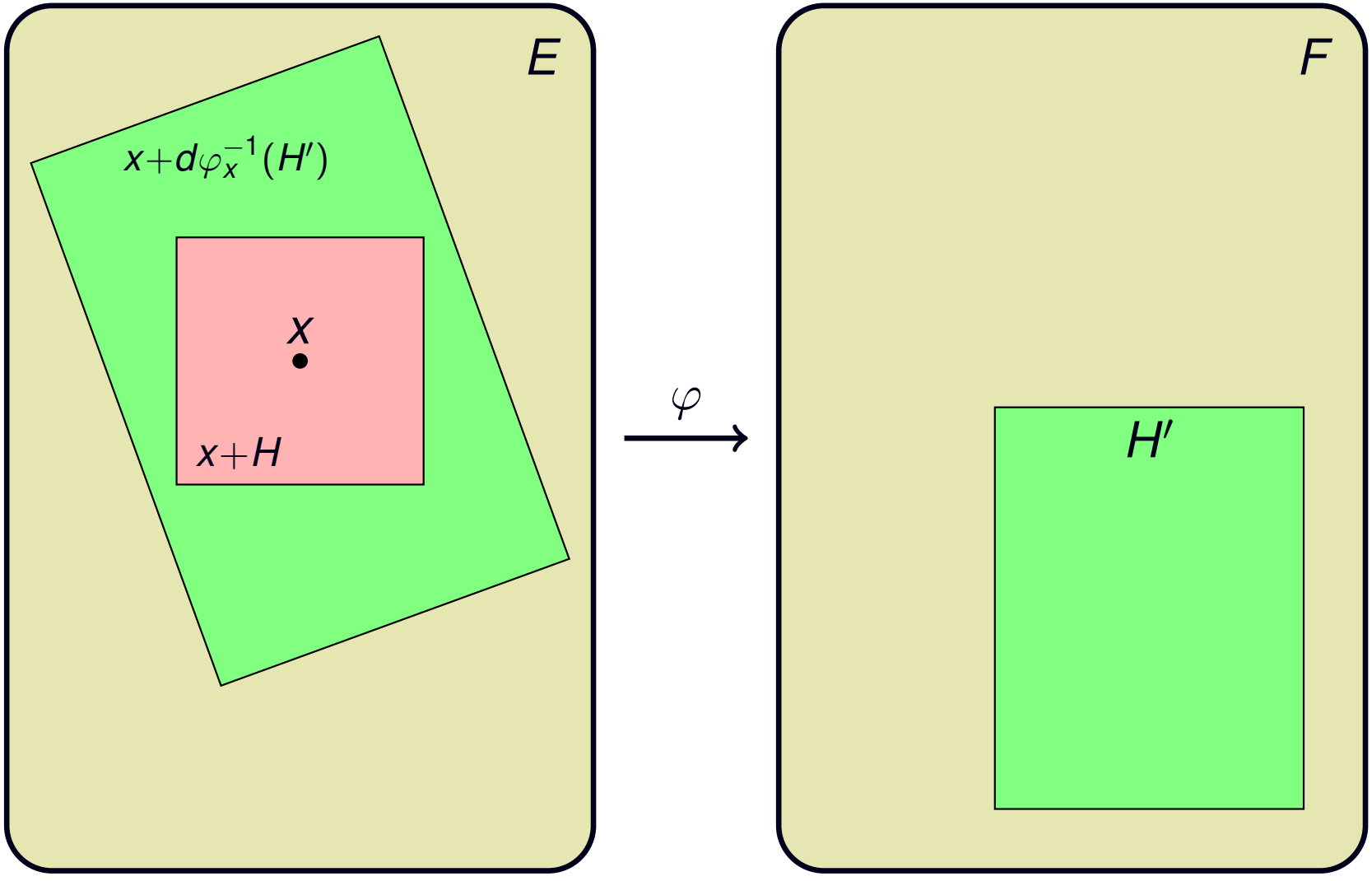
Contexte de l'arithmétique paresseuse



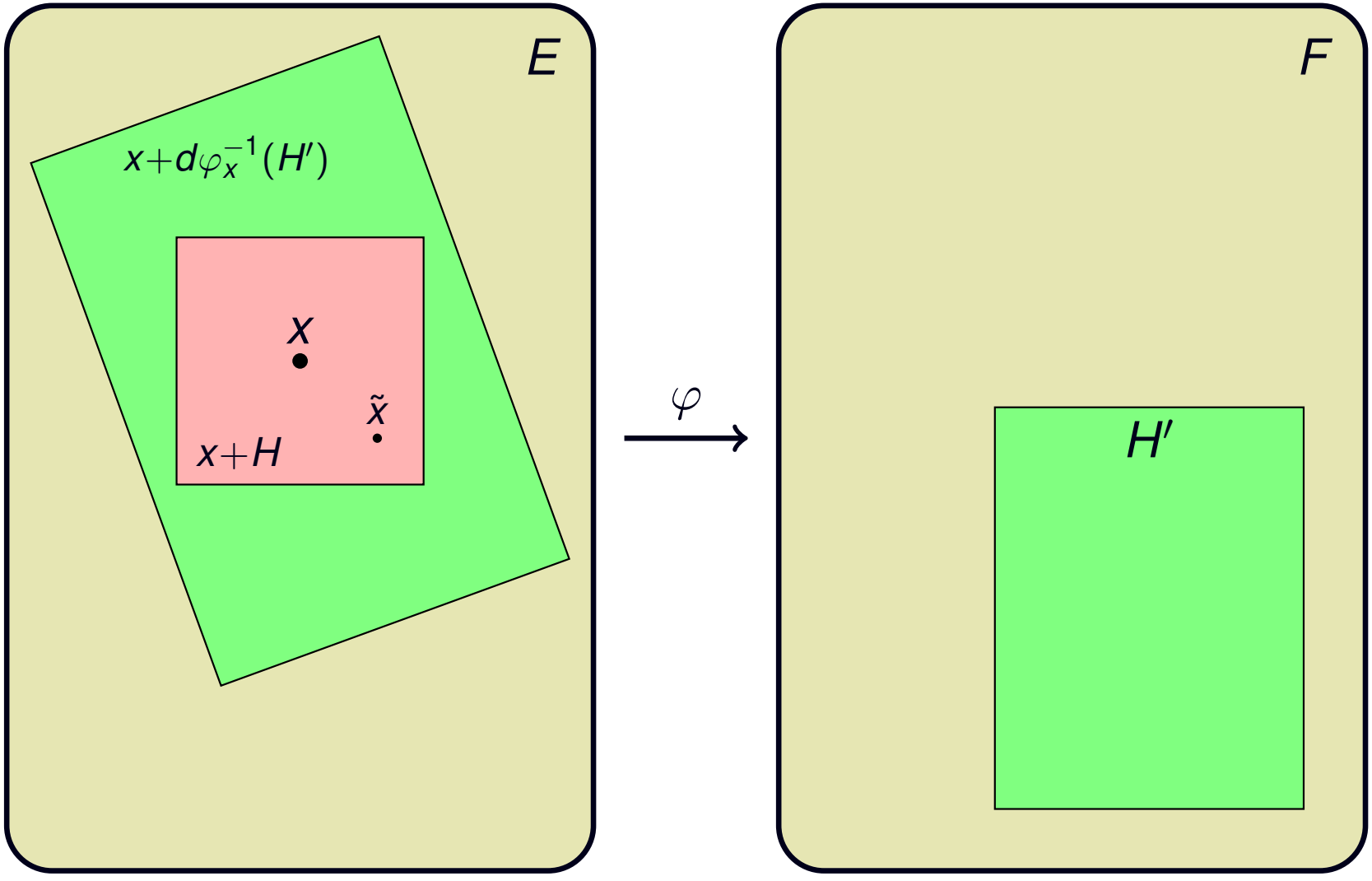
La méthode de la précision adaptative
Contexte de l'arithmétique paresseuse



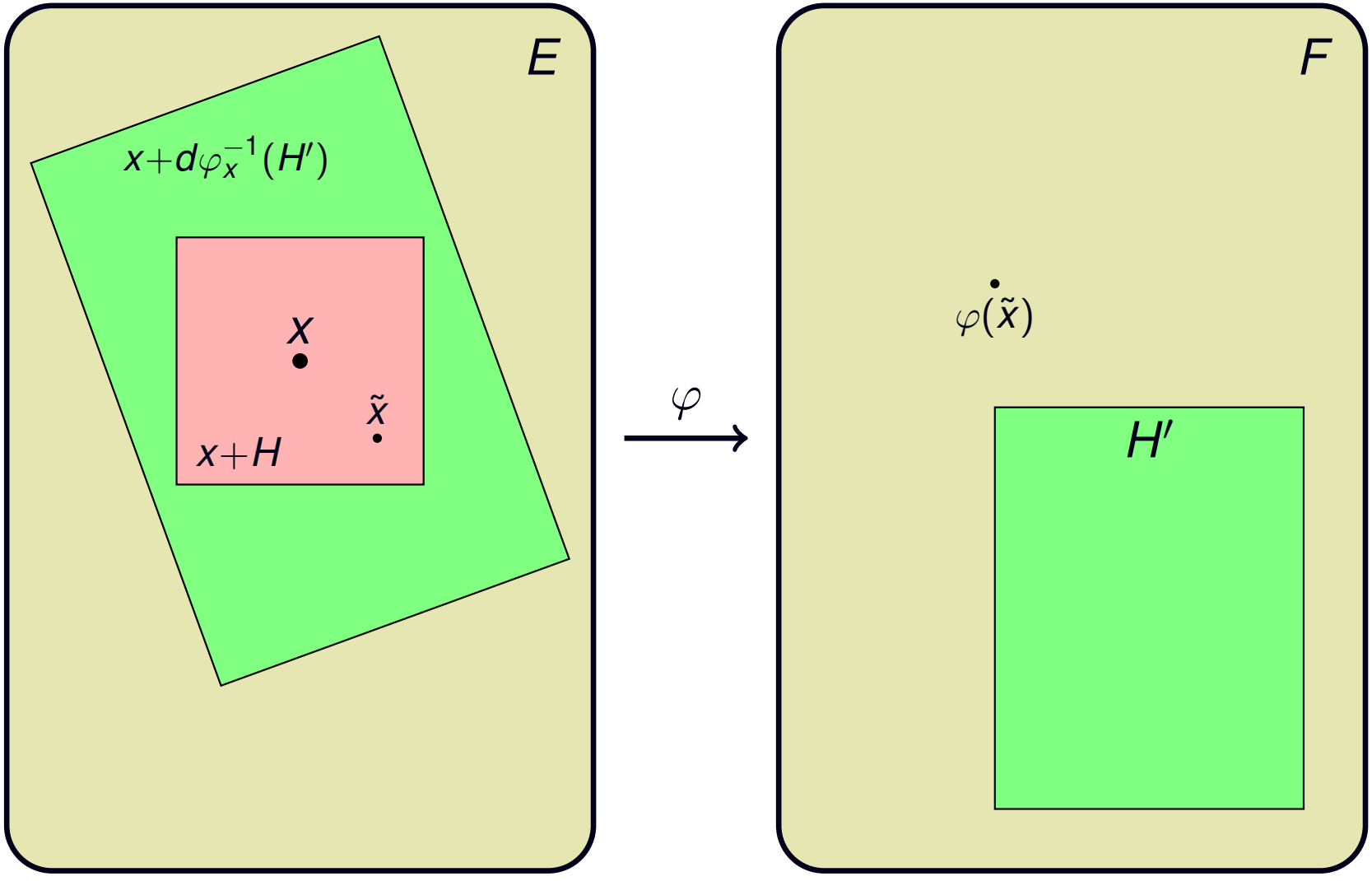
La méthode de la précision adaptative
Contexte de l'arithmétique paresseuse



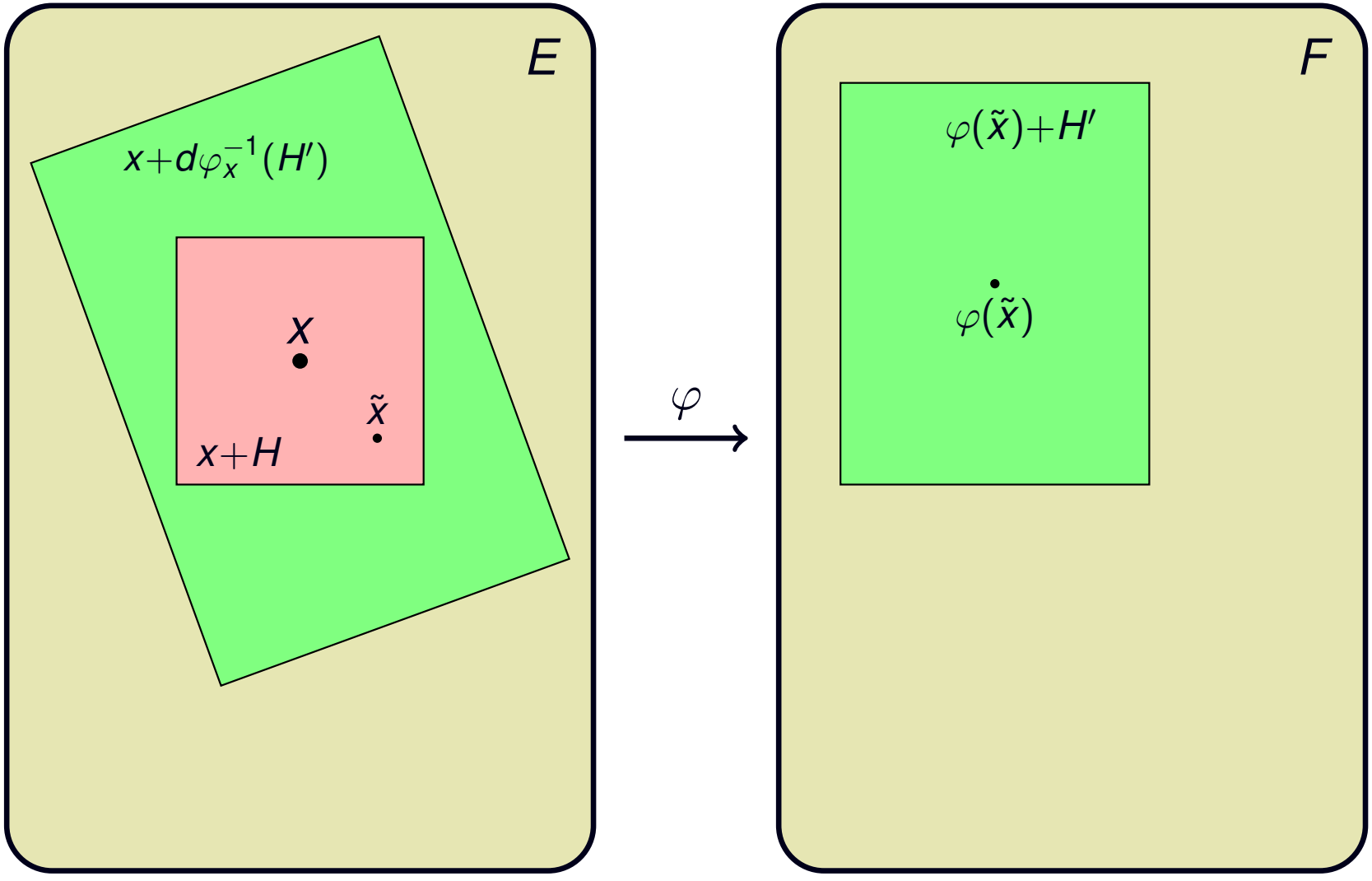
La méthode de la précision adaptative
Contexte de l'arithmétique paresseuse



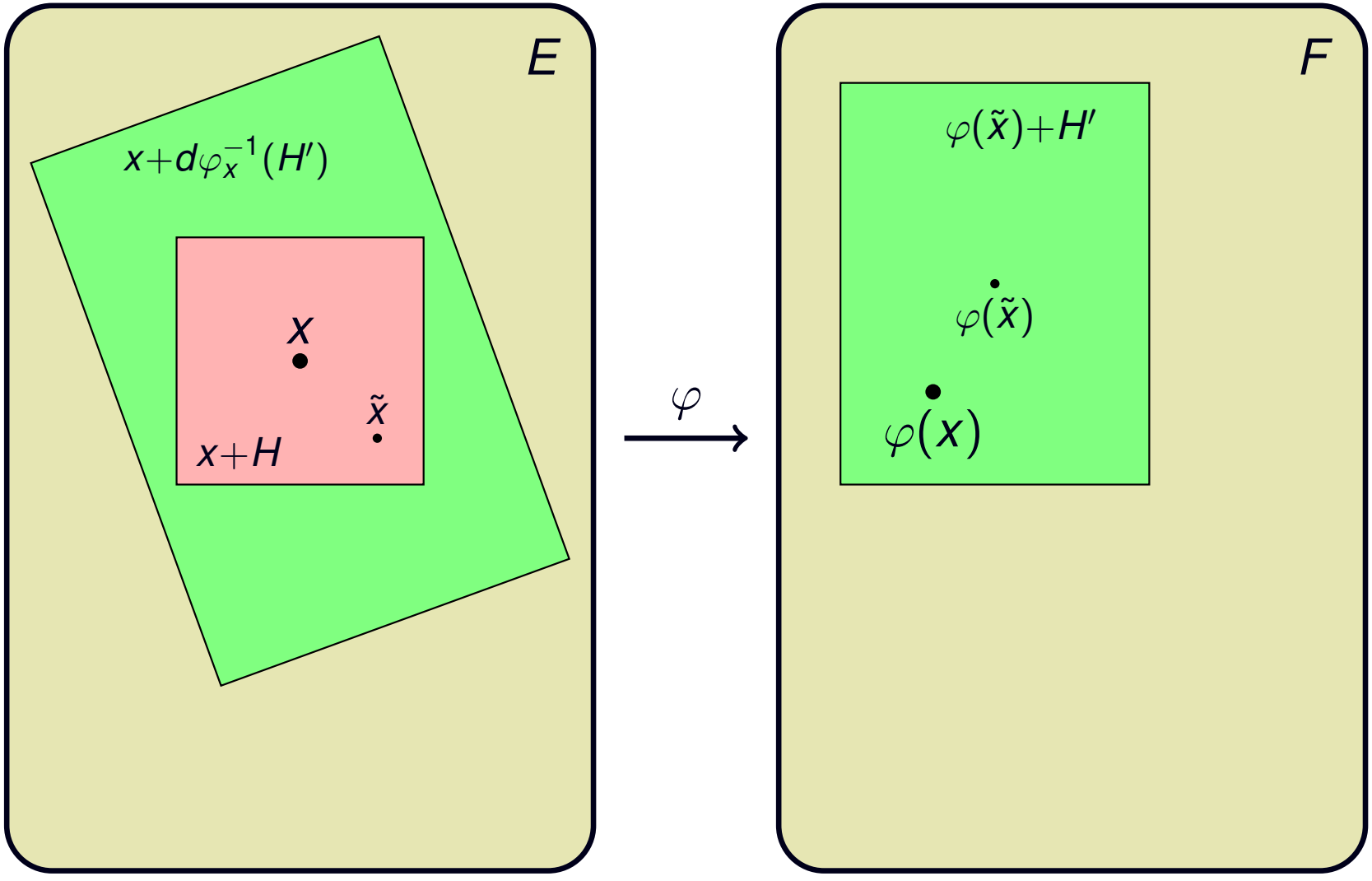
La méthode de la précision adaptative
Contexte de l'arithmétique paresseuse



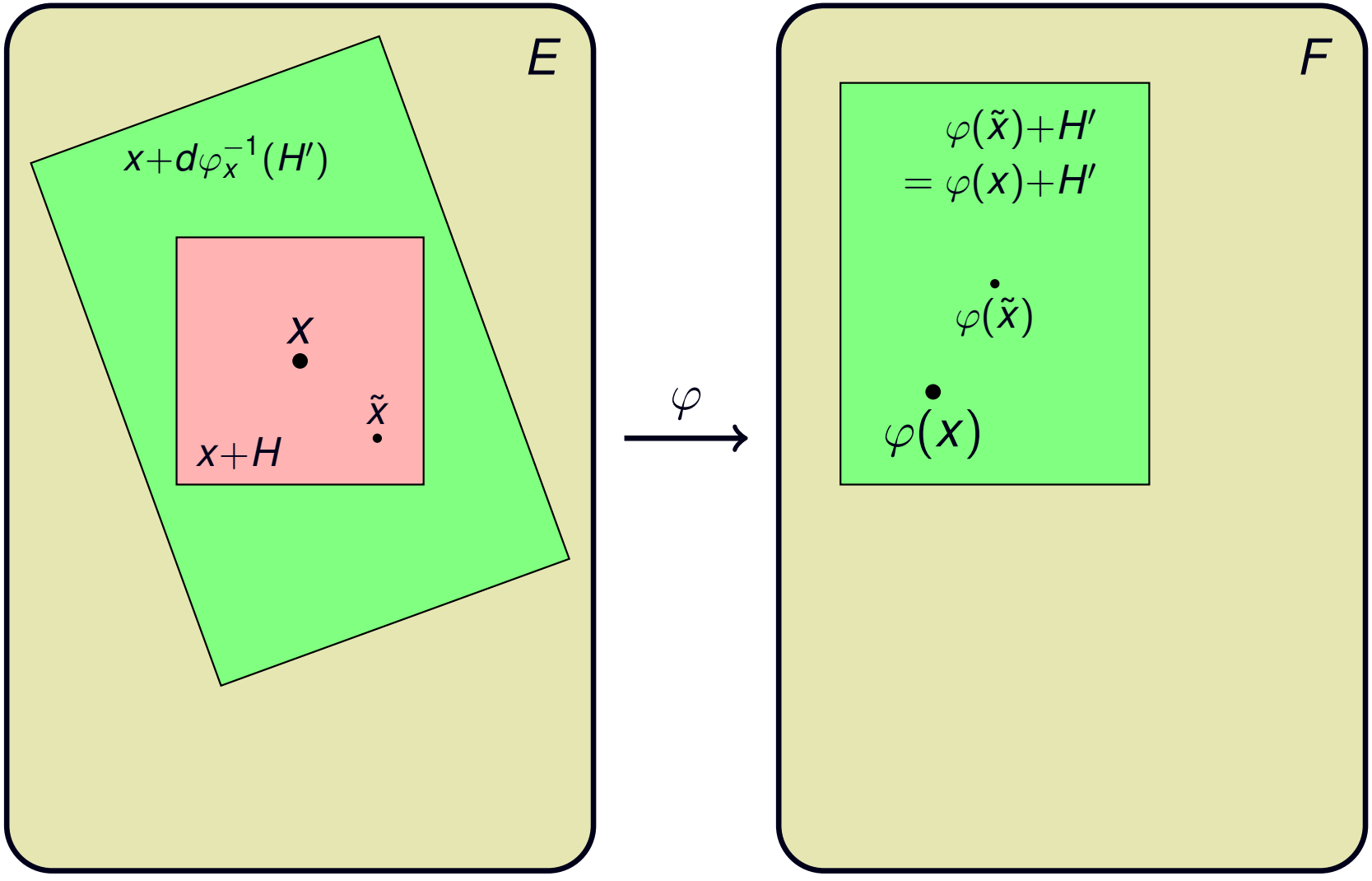
La méthode de la précision adaptative
Contexte de l'arithmétique paresseuse



La méthode de la précision adaptative
Contexte de l'arithmétique paresseuse



La méthode de la précision adaptative
Contexte de l'arithmétique paresseuse



La méthode de la précision adaptative

Contexte de l'arithmétique paresseuse

```
def Phi_stabilized_v1(x):
    # Cas où H' = p^N Z_p
    def Phi_of_x(N):
        xapp = x(p^N H)
        return Phi(xapp) % p^N
    return Phi_of_x
```

La méthode de la précision adaptative

Contexte de l'arithmétique paresseuse

```
def Phi_stabilized_v2(x):
    # Cas où H' = p^N Z_p
    def Phi_of_x(N):
        y_0 = x(p^N H_{0,min})
        for i in 1,2,...,n:
            y_i = Step_i(y_{i-1}) % p^N H_{i,min}
        return y_n % p^N
    return Phi_of_x
```

Exemple : la suite de Somos 4

$$u_1 = a, \quad u_2 = b, \quad u_3 = c, \quad u_4 = d$$

$$u_{n+4} = \frac{u_{n+1}u_{n+3} + u_{n+2}^2}{u_n}$$

Phénomène de Laurent

$$u_5 = \frac{1}{a}\left(c^2 + bd\right)$$

$$u_6 = \frac{1}{ab}\left(c^3 + bcd + ad^2\right)$$

$$u_7 = \frac{1}{a^2bc}\left(bc^4 + 2b^2c^2d + ac^3d + b^3d^2 + abcd^2 + a^2d^3\right)$$

$$u_8 = \frac{1}{a^3b^2cd}\left(b^2c^6 + ac^7 + 3b^3c^4d + 3abc^5d + 3b^4c^2d^2 + 3ab^2c^3d^2 + 2a^2c^4d^2 + b^5d^3 + ab^3cd^3 + 3a^2bc^2d^3 + a^2b^2d^4 + a^3cd^4\right)$$

$$u_9 = \frac{1}{a^3b^2c^2d}\left(b^2c^8 + ac^9 + 4b^3c^6d + 3abc^7d + 6b^4c^4d^2 + 6ab^2c^5d^2 + 3a^2c^6d^2 + 4b^5c^2d^3 + 7ab^3c^3d^3 + 6a^2bc^4d^3 + b^6d^4 + 3ab^4cd^4 + 5a^2b^2c^2d^4 + 3a^3c^3d^4 + 2a^2b^3d^5 + 3a^3bcd^5 + a^4d^6\right)$$

Exemple : la suite de Somos 4

$$
\begin{aligned}
u_5 &= \frac{1}{a}\left(c^2+bd\right)\\
u_6 &= \frac{1}{ab}\left(c^3+bcd+ad^2\right)\\
u_7 &= \frac{1}{a^2bc}\left(bc^4+2b^2c^2d+ac^3d+b^3d^2+abcd^2+a^2d^3\right)\\
u_8 &= \frac{1}{a^3b^2cd}\left(b^2c^6+ac^7+3b^3c^4d+3abc^5d+3b^4c^2d^2+3ab^2c^3d^2\right.\\
&\qquad \left.+2a^2c^4d^2+b^5d^3+ab^3cd^3+3a^2bc^2d^3+a^2b^2d^4+a^3cd^4\right)\\
u_9 &= \frac{1}{a^3b^2c^2d}\left(b^2c^8+ac^9+4b^3c^6d+3abc^7d+6b^4c^4d^2+6ab^2c^5d^2\right.\\
&\qquad +3a^2c^6d^2+4b^5c^2d^3+7ab^3c^3d^3+6a^2bc^4d^3+b^6d^4\\
&\qquad \left.+3ab^4cd^4+5a^2b^2c^2d^4+3a^3c^3d^4+2a^2b^3d^5+3a^3bcd^5+a^4d^6\right)
\end{aligned}
$$

Exemple : la suite de Somos 4

$$
\begin{aligned}
u_5 &= \frac{1}{a}\left(c^2+bd\right)\\
u_6 &= \frac{1}{ab}\left(c^3+bcd+ad^2\right)\\
u_7 &= \frac{1}{a^2bc}\left(bc^4+2b^2c^2d+ac^3d+b^3d^2+abcd^2+a^2d^3\right)\\
u_8 &= \frac{1}{a^3b^2cd}\left(b^2c^6+ac^7+3b^3c^4d+3abc^5d+3b^4c^2d^2+3ab^2c^3d^2\right.\\
&\qquad \left.+2a^2c^4d^2+b^5d^3+ab^3cd^3+3a^2bc^2d^3+a^2b^2d^4+a^3cd^4\right)\\
u_9 &= \frac{1}{a^3b^2c^2d}\left(b^2c^8+ac^9+4b^3c^6d+3abc^7d+6b^4c^4d^2+6ab^2c^5d^2\right.\\
&\qquad +3a^2c^6d^2+4b^5c^2d^3+7ab^3c^3d^3+6a^2bc^4d^3+b^6d^4\\
&\qquad \left.+3ab^4cd^4+5a^2b^2c^2d^4+3a^3c^3d^4+2a^2b^3d^5+3a^3bcd^5+a^4d^6\right)\\
u_{10} &= \frac{1}{a^5b^3c^3d^2}\left(b^4c^{10}+2ab^2c^{11}+a^2c^{12}+5b^5c^8d+11ab^3c^9d+6a^2bc^{10}d\right.\\
&\qquad +10b^6c^6d^2+24ab^4c^7d^2+17a^2b^2c^8d^2+4a^3c^9d^2\\
&\qquad +10b^7c^4d^3+26ab^5c^5d^3+28a^2b^3c^6d^3+15a^3bc^7d^3\\
&\qquad +5b^8c^2d^4+14ab^6c^3d^4+27a^2b^4c^4d^4+24a^3b^2c^5d^4\\
&\qquad +6a^4c^6d^4+b^9d^5+3ab^7cd^5+14a^2b^5c^2d^5+19a^3b^3c^3d^5\\
&\qquad +12a^4bc^4d^5+3a^2b^6d^6+6a^3b^4cd^6+9a^4b^2c^2d^6\\
&\qquad \left.+4a^5c^3d^6+3a^4b^3d^7+3a^5bcd^7+a^6d^8\right)
\end{aligned}
$$

Exemple : la suite de Somos 4

Évaluation de la suite de Somos 4

```
def somos1(a,b,c,d,n):
    x,y,z,t = a,b,c,d
    for i in 1,2,...,n-4:
        x,y,z,t = y, z, t, (y*t + z*z)/x
    return t

def somos2(a,b,c,d,n):
    X,Y,Z,T = A,B,C,D
    for i in 1,2,...,n-4:
        X,Y,Z,T = Y, Z, T, (Y*T + Z*Z)/X
    return T(A=a, B=b, C=c, D=d)
```

Exemple : la suite de Somos 4

Exemple : la suite de Somos 4

u_1 ... 0000000001

u_2 ... 0000000001

u_3 ... 0000000001

u_4 ... 0000000001

Exemple : la suite de Somos 4

	Laurent method
u_1	$\ldots 0000000001$
u_2	$\ldots 0000000001$
u_3	$\ldots 0000000001$
u_4	$\ldots 0000000001$
u_5	$\ldots 0000000010$
u_6	$\ldots 0000000011$
u_7	$\ldots 0000000111$
u_8	$\ldots 0000010111$
u_9	$\ldots 0000111011$
u_{10}	$\ldots 0100111010$

Exemple : la suite de Somos 4

	Laurent method
u_1	...0000000001
u_2	...0000000001
u_3	...0000000001
u_4	...0000000001
u_5	...0000000010
u_6	...0000000011
u_7	...0000000111
u_8	...0000010111
u_9	...0000111011
u_{10}	...0100111010
u_{50}	...0000011010
u_{500}	...1111110010

Exemple : la suite de Somos 4

	Laurent method	Zealous arith.
u_1	...0000000001	...0000000001
u_2	...0000000001	...0000000001
u_3	...0000000001	...0000000001
u_4	...0000000001	...0000000001
u_5	...0000000010	
u_6	...0000000011	
u_7	...0000000111	
u_8	...0000010111	
u_9	...0000111011	
u_{10}	...0100111010	
u_{50}	...0000011010	
u_{500}	...1111110010	

Exemple : la suite de Somos 4

	Laurent method	Zealous arith.
u_1	...0000000001	...0000000001
u_2	...0000000001	...0000000001
u_3	...0000000001	...0000000001
u_4	...0000000001	...0000000001
u_5	...0000000010	...0000000010
u_6	...0000000011	
u_7	...0000000111	
u_8	...0000010111	
u_9	...0000111011	
u_{10}	...0100111010	
u_{50}	...0000011010	
u_{500}	...1111110010	

Exemple : la suite de Somos 4

	Laurent method	Zealous arith.
u_1	...0000000001	...0000000001
u_2	...0000000001	...0000000001
u_3	...0000000001	...0000000001
u_4	...0000000001	...0000000001
u_5	...0000000010	...0000000010
u_6	...0000000011	...0000000011
u_7	...0000000111	
u_8	...0000010111	
u_9	...0000111011	
u_{10}	...0100111010	
u_{50}	...0000011010	
u_{500}	...1111110010	

Exemple : la suite de Somos 4

	Laurent method	Zealous arith.
u_1	...0000000001	...0000000001
u_2	...0000000001	...0000000001
u_3	...0000000001	...0000000001
u_4	...0000000001	...0000000001
u_5	...0000000010	...0000000010
u_6	...0000000011	...0000000011
u_7	...0000000111	...0000000111
u_8	...0000010111	
u_9	...0000111011	
u_{10}	...0100111010	
u_{50}	...0000011010	
u_{500}	...1111110010	

Exemple : la suite de Somos 4

	Laurent method	Zealous arith.
u_1	...0000000001	...0000000001
u_2	...0000000001	...0000000001
u_3	...0000000001	...0000000001
u_4	...0000000001	...0000000001
u_5	...0000000010	...0000000010
u_6	...0000000011	...0000000011
u_7	...0000000111	...0000000111
u_8	...0000010111	...0000010111
u_9	...0000111011	
u_{10}	...0100111010	
u_{50}	...0000011010	
u_{500}	...1111110010	

Exemple : la suite de Somos 4

	Laurent method	Zealous arith.
u_1	...0000000001	...0000000001
u_2	...0000000001	...0000000001
u_3	...0000000001	...0000000001
u_4	...0000000001	...0000000001
u_5	...0000000010	...0000000010
u_6	...0000000011	...0000000011
u_7	...0000000111	...0000000111
u_8	...0000010111	...0000010111
u_9	...0000111011	...000111011
u_{10}	...0100111010	
u_{50}	...0000011010	
u_{500}	...1111110010	

Exemple : la suite de Somos 4

	Laurent method	Zealous arith.
u_1	...0000000001	...0000000001
u_2	...0000000001	...0000000001
u_3	...0000000001	...0000000001
u_4	...0000000001	...0000000001
u_5	...0000000010	...0000000010
u_6	...0000000011	...0000000011
u_7	...0000000111	...0000000111
u_8	...0000010111	...0000010111
u_9	...0000111011	...000111011
u_{10}	...0100111010	...100111010
u_{50}	...0000011010	
u_{500}	...1111110010	

Exemple : la suite de Somos 4

	Laurent method	Zealous arith.
u_1	...0000000001	...0000000001
u_2	...0000000001	...0000000001
u_3	...0000000001	...0000000001
u_4	...0000000001	...0000000001
u_5	...0000000010	...0000000010
u_6	...0000000011	...0000000011
u_7	...0000000111	...0000000111
u_8	...0000010111	...0000010111
u_9	...0000111011	...000111011
u_{10}	...0100111010	...100111010
u_{50}	...0000011010	...0
u_{500}	...1111110010	

Exemple : la suite de Somos 4

	Laurent method	Zealous arith.
u_1	...0000000001	...0000000001
u_2	...0000000001	...0000000001
u_3	...0000000001	...0000000001
u_4	...0000000001	...0000000001
u_5	...0000000010	...0000000010
u_6	...0000000011	...0000000011
u_7	...0000000111	...0000000111
u_8	...0000010111	...0000010111
u_9	...0000111011	...000111011
u_{10}	...0100111010	...100111010
u_{50}	...0000011010	...0
u_{54}	...0100101001	**BOUM**
u_{500}	...1111110010	

Exemple : la suite de Somos 4

	Laurent method	Zealous arith.
u_1	...0000000001	...0000000001
u_2	...0000000001	...0000000001
u_3	...0000000001	...0000000001
u_4	...0000000001	...0000000001
u_5	...0000000010	...0000000010
u_6	...0000000011	...0000000011
u_7	...0000000111	...0000000111
u_8	...0000010111	...0000010111
u_9	...0000111011	...000111011
u_{10}	...0100111010	...100111010
u_{50}	...0000011010	...0
u_{54}	...0100101001	**BOUM**
u_{500}	...1111110010	—

Exemple : la suite de Somos 4

	Laurent method	Zealous arith.	Float. arith.
u_1	...0000000001	...0000000001	...0000000001
u_2	...0000000001	...0000000001	...0000000001
u_3	...0000000001	...0000000001	...0000000001
u_4	...0000000001	...0000000001	...0000000001
u_5	...0000000010	...0000000010	
u_6	...0000000011	...0000000011	
u_7	...0000000111	...0000000111	
u_8	...0000010111	...0000010111	
u_9	...0000111011	...000111011	
u_{10}	...0100111010	...100111010	
u_{50}	...0000011010	...0	
u_{54}	...0100101001	**BOUM**	
u_{500}	...1111110010	—	

Exemple : la suite de Somos 4

	Laurent method	Zealous arith.	Float. arith.
u_1	...0000000001	...0000000001	...0000000001
u_2	...0000000001	...0000000001	...0000000001
u_3	...0000000001	...0000000001	...0000000001
u_4	...0000000001	...0000000001	...0000000001
u_5	...0000000010	...0000000010	...0000000010
u_6	...0000000011	...0000000011	...0000000011
u_7	...0000000111	...0000000111	...0000000111
u_8	...0000010111	...0000010111	...0000010111
u_9	...0000111011	...000111011	...0000111011
u_{10}	...0100111010	...100111010	...10100111010
u_{50}	...0000011010	...0	...11000011010
u_{54}	...0100101001	**BOUM**	...1100101001
u_{500}	...1111110010	—	...01111110010

Exemple : la suite de Somos 4

	Laurent method	Zealous arith.	Float. arith.	Relaxed arith.
u_1	...0000000001	...0000000001	...0000000001	
u_2	...0000000001	...0000000001	...0000000001	
u_3	...0000000001	...0000000001	...0000000001	
u_4	...0000000001	...0000000001	...0000000001	
u_5	...0000000010	...0000000010	...0000000010	
u_6	...0000000011	...0000000011	...0000000011	
u_7	...0000000111	...0000000111	...0000000111	
u_8	...0000010111	...0000010111	...0000010111	
u_9	...0000111011	...000111011	...0000111011	
u_{10}	...0100111010	...100111010	...10100111010	
u_{50}	...0000011010	...0	...11000011010	
u_{54}	...0100101001	**BOUM**	...1100101001	
u_{500}	...1111110010	—	...01111110010	

Exemple : la suite de Somos 4

	Laurent method	Zealous arith.	Float. arith.	Relaxed arith.
u_1	...0000000001	...0000000001	...0000000001	—
u_2	...0000000001	...0000000001	...0000000001	—
u_3	...0000000001	...0000000001	...0000000001	—
u_4	...0000000001	...0000000001	...0000000001	—
u_5	...0000000010	...0000000010	...0000000010	
u_6	...0000000011	...0000000011	...0000000011	
u_7	...0000000111	...0000000111	...0000000111	
u_8	...0000010111	...0000010111	...0000010111	
u_9	...0000111011	...000111011	...0000111011	
u_{10}	...0100111010	...100111010	...10100111010	
u_{50}	...0000011010	...0	...11000011010	
u_{54}	...0100101001	**BOUM**	...1100101001	
u_{500}	...1111110010	—	...01111110010	

Exemple : la suite de Somos 4

	Laurent method	Zealous arith.	Float. arith.	Relaxed arith.
u_1	...0000000001	...0000000001	...0000000001	—
u_2	...0000000001	...0000000001	...0000000001	—
u_3	...0000000001	...0000000001	...0000000001	—
u_4	...0000000001	...0000000001	...0000000001	—
u_5	...0000000010	...0000000010	...0000000010	precision on u_1 : 10
u_6	...0000000011	...0000000011	...0000000011	
u_7	...0000000111	...0000000111	...0000000111	
u_8	...0000010111	...0000010111	...0000010111	
u_9	...0000111011	...000111011	...0000111011	
u_{10}	...0100111010	...100111010	...10100111010	
u_{50}	...0000011010	...0	...11000011010	
u_{54}	...0100101001	**BOUM**	...1100101001	
u_{500}	...1111110010	—	...01111110010	

Exemple : la suite de Somos 4

	Laurent method	Zealous arith.	Float. arith.	Relaxed arith.
u_1	...0000000001	...0000000001	...0000000001	—
u_2	...0000000001	...0000000001	...0000000001	—
u_3	...0000000001	...0000000001	...0000000001	—
u_4	...0000000001	...0000000001	...0000000001	—
u_5	...0000000010	...0000000010	...0000000010	precision on u_1 : 10
u_6	...0000000011	...0000000011	...0000000011	precision on u_1 : 10
u_7	...0000000111	...0000000111	...0000000111	
u_8	...0000010111	...0000010111	...0000010111	
u_9	...0000111011	...000111011	...0000111011	
u_{10}	...0100111010	...100111010	...10100111010	
u_{50}	...0000011010	...0	...11000011010	
u_{54}	...0100101001	**BOUM**	...1100101001	
u_{500}	...1111110010	—	...01111110010	

Exemple : la suite de Somos 4

	Laurent method	Zealous arith.	Float. arith.	Relaxed arith.
u_1	...0000000001	...0000000001	...0000000001	—
u_2	...0000000001	...0000000001	...0000000001	—
u_3	...0000000001	...0000000001	...0000000001	—
u_4	...0000000001	...0000000001	...0000000001	—
u_5	...0000000010	...0000000010	...0000000010	precision on u_1 : 10
u_6	...0000000011	...0000000011	...0000000011	precision on u_1 : 10
u_7	...0000000111	...0000000111	...0000000111	precision on u_1 : 10
u_8	...0000010111	...0000010111	...0000010111	
u_9	...0000111011	...000111011	...0000111011	
u_{10}	...0100111010	...100111010	...10100111010	
u_{50}	...0000011010	...0	...11000011010	
u_{54}	...0100101001	**BOUM**	...1100101001	
u_{500}	...1111110010	—	...01111110010	

Exemple : la suite de Somos 4

	Laurent method	Zealous arith.	Float. arith.	Relaxed arith.
u_1	...0000000001	...0000000001	...0000000001	—
u_2	...0000000001	...0000000001	...0000000001	—
u_3	...0000000001	...0000000001	...0000000001	—
u_4	...0000000001	...0000000001	...0000000001	—
u_5	...0000000010	...0000000010	...0000000010	precision on u_1 : 10
u_6	...0000000011	...0000000011	...0000000011	precision on u_1 : 10
u_7	...0000000111	...0000000111	...0000000111	precision on u_1 : 10
u_8	...0000010111	...0000010111	...0000010111	precision on u_1 : 10
u_9	...0000111011	...000111011	...0000111011	
u_{10}	...0100111010	...100111010	...10100111010	
u_{50}	...0000011010	...0	...11000011010	
u_{54}	...0100101001	**BOUM**	...1100101001	
u_{500}	...1111110010	—	...01111110010	

Exemple : la suite de Somos 4

	Laurent method	Zealous arith.	Float. arith.	Relaxed arith.
u_1	...0000000001	...0000000001	...0000000001	—
u_2	...0000000001	...0000000001	...0000000001	—
u_3	...0000000001	...0000000001	...0000000001	—
u_4	...0000000001	...0000000001	...0000000001	—
u_5	...0000000010	...0000000010	...0000000010	precision on u_1 : 10
u_6	...0000000011	...0000000011	...0000000011	precision on u_1 : 10
u_7	...0000000111	...0000000111	...0000000111	precision on u_1 : 10
u_8	...0000010111	...0000010111	...0000010111	precision on u_1 : 10
u_9	...0000111011	...000111011	...0000111011	precision on u_1 : 11
u_{10}	...0100111010	...100111010	...10100111010	
u_{50}	...0000011010	...0	...11000011010	
u_{54}	...0100101001	**BOUM**	...1100101001	
u_{500}	...1111110010	—	...01111110010	

Exemple : la suite de Somos 4

	Laurent method	Zealous arith.	Float. arith.	Relaxed arith.
u_1	...0000000001	...0000000001	...0000000001	—
u_2	...0000000001	...0000000001	...0000000001	—
u_3	...0000000001	...0000000001	...0000000001	—
u_4	...0000000001	...0000000001	...0000000001	—
u_5	...0000000010	...0000000010	...0000000010	precision on u_1 : 10
u_6	...0000000011	...0000000011	...0000000011	precision on u_1 : 10
u_7	...0000000111	...0000000111	...0000000111	precision on u_1 : 10
u_8	...0000010111	...0000010111	...0000010111	precision on u_1 : 10
u_9	...0000111011	...000111011	...0000111011	precision on u_1 : 11
u_{10}	...0100111010	...100111010	...10100111010	precision on u_1 : 11
u_{50}	...0000011010	...0	...11000011010	
u_{54}	...0100101001	**BOUM**	...1100101001	
u_{500}	...1111110010	—	...01111110010	

Exemple : la suite de Somos 4

	Laurent method	Zealous arith.	Float. arith.	Relaxed arith.
u_1	...0000000001	...0000000001	...0000000001	—
u_2	...0000000001	...0000000001	...0000000001	—
u_3	...0000000001	...0000000001	...0000000001	—
u_4	...0000000001	...0000000001	...0000000001	—
u_5	...0000000010	...0000000010	...0000000010	precision on u_1 : 10
u_6	...0000000011	...0000000011	...0000000011	precision on u_1 : 10
u_7	...0000000111	...0000000111	...0000000111	precision on u_1 : 10
u_8	...0000010111	...0000010111	...0000010111	precision on u_1 : 10
u_9	...0000111011	...000111011	...0000111011	precision on u_1 : 11
u_{10}	...0100111010	...100111010	...10100111010	precision on u_1 : 11
u_{50}	...0000011010	...0	...11000011010	precision on u_1 : 19
u_{54}	...0100101001	**BOUM**	...1100101001	
u_{500}	...1111110010	—	...01111110010	

Exemple : la suite de Somos 4

	Laurent method	Zealous arith.	Float. arith.	Relaxed arith.
u_1	...0000000001	...0000000001	...0000000001	—
u_2	...0000000001	...0000000001	...0000000001	—
u_3	...0000000001	...0000000001	...0000000001	—
u_4	...0000000001	...0000000001	...0000000001	—
u_5	...0000000010	...0000000010	...0000000010	precision on u_1 : 10
u_6	...0000000011	...0000000011	...0000000011	precision on u_1 : 10
u_7	...0000000111	...0000000111	...0000000111	precision on u_1 : 10
u_8	...0000010111	...0000010111	...0000010111	precision on u_1 : 10
u_9	...0000111011	...000111011	...0000111011	precision on u_1 : 11
u_{10}	...0100111010	...100111010	...10100111010	precision on u_1 : 11
u_{50}	...0000011010	...0	...11000011010	precision on u_1 : 19
u_{54}	...0100101001	**BOUM**	...1100101001	precision on u_1 : 20
u_{500}	...1111110010	—	...01111110010	

Exemple : la suite de Somos 4

	Laurent method	Zealous arith.	Float. arith.	Relaxed arith.
u_1	...0000000001	...0000000001	...0000000001	—
u_2	...0000000001	...0000000001	...0000000001	—
u_3	...0000000001	...0000000001	...0000000001	—
u_4	...0000000001	...0000000001	...0000000001	—
u_5	...0000000010	...0000000010	...0000000010	precision on u_1 : 10
u_6	...0000000011	...0000000011	...0000000011	precision on u_1 : 10
u_7	...0000000111	...0000000111	...0000000111	precision on u_1 : 10
u_8	...0000010111	...0000010111	...0000010111	precision on u_1 : 10
u_9	...0000111011	...000111011	...0000111011	precision on u_1 : 11
u_{10}	...0100111010	...100111010	...10100111010	precision on u_1 : 11
u_{50}	...0000011010	...0	...11000011010	precision on u_1 : 19
u_{54}	...0100101001	**BOUM**	...1100101001	precision on u_1 : 20
u_{500}	...1111110010	—	...01111110010	precision on u_1 : 109

Exemple : la suite de Somos 4

Exemple : la suite de Somos 4

	Laurent method	Zealous arith.	Float. arith.	Relaxed arith.
u_1	...0000000001	...0000000001	...0000000001	—
u_2	...0000000001	...0000000001	...0000000001	—
u_3	...0000000001	...0000000001	...0000000001	—
u_4	...0000000011	...0000000011	...0000000011	—
u_5	...0000000100	...0000000100	...00000000100	precision on u_1 : 10
u_6	...0000001101	...0000001101	...0000001101	precision on u_1 : 10
u_7	...0000110111	...0000110111	...0000110111	precision on u_1 : 10
u_8	...0111010111	...0111010111	...0111010111	precision on u_1 : 10
u_9	...0111101111	...11101111	...1111101111	precision on u_1 : 12
u_{10}	...0000010010	...00010010	...11000010010	precision on u_1 : 12
u_{11}	...1000111001	...00111001	...0000111001	precision on u_1 : 12
u_{12}	...0011111101	...11111101	...0011111101	precision on u_1 : 12
u_{13}	...0000110101	...00110101	...0000110101	precision on u_1 : 12
u_{14}	...1101010011	...1010011	...1101010011	precision on u_1 : 13
u_{15}	...0000000000	...0000000	0	precision on u_1 : 13
u_{16}	...0101011101	...1011101	...0101011101	precision on u_1 : 13
u_{17}	...1001101011	...1101011	...1001101011	precision on u_1 : 13
u_{18}	...0011110011	...1110011	...0011110011	precision on u_1 : 13
u_{19}	...0000000111	**BOUM**	**BOUM**	precision on u_1 : 23

Exemple : la suite de Somos 4

Exemple : la suite de Somos 4

$$\begin{array}{rccc} \sigma : & \mathbb{Q}_p^4 & \longrightarrow & \mathbb{Q}_p^4 \\ & (x,y,z,t) & \mapsto & \left(y,t,z,\frac{yt+z^2}{x}\right) \end{array}$$

$$J(\sigma)_{(x,y,z,t)} = \begin{pmatrix} 0 & 0 & 0 & -\frac{yt+z^2}{x^2} \\ 1 & 0 & 0 & \frac{t}{x} \\ 0 & 1 & 0 & \frac{2z}{x} \\ 0 & 0 & 1 & \frac{y}{x} \end{pmatrix}$$

$$\det J(\sigma^i)_{(a,b,c,d)} = \frac{u_{i+1}u_{i+2}u_{i+3}u_{i+4}}{abcd} = p^{v(i)} \times (\text{inversible})$$

$$J(\sigma^i)_{(a,b,c,d)} \in M_4(\mathbb{Z}_p)$$

$$p^{v(i)}\mathbb{Z}_p^4 \subset d\sigma^i_{(a,b,c,d)}\left(\mathbb{Z}_p^4\right) \subset \mathbb{Z}_p^4$$

Exemple : la suite de Somos 4

Exemple : la suite de Somos 4

$$p^{N+v(i)}\mathbb{Z}_p^4 \quad \subset \quad d\sigma^i_{(a,b,c,d)}\left(p^N\mathbb{Z}_p^4\right) \quad \subset \quad p^N\mathbb{Z}_p^4$$

Exemple : la suite de Somos 4

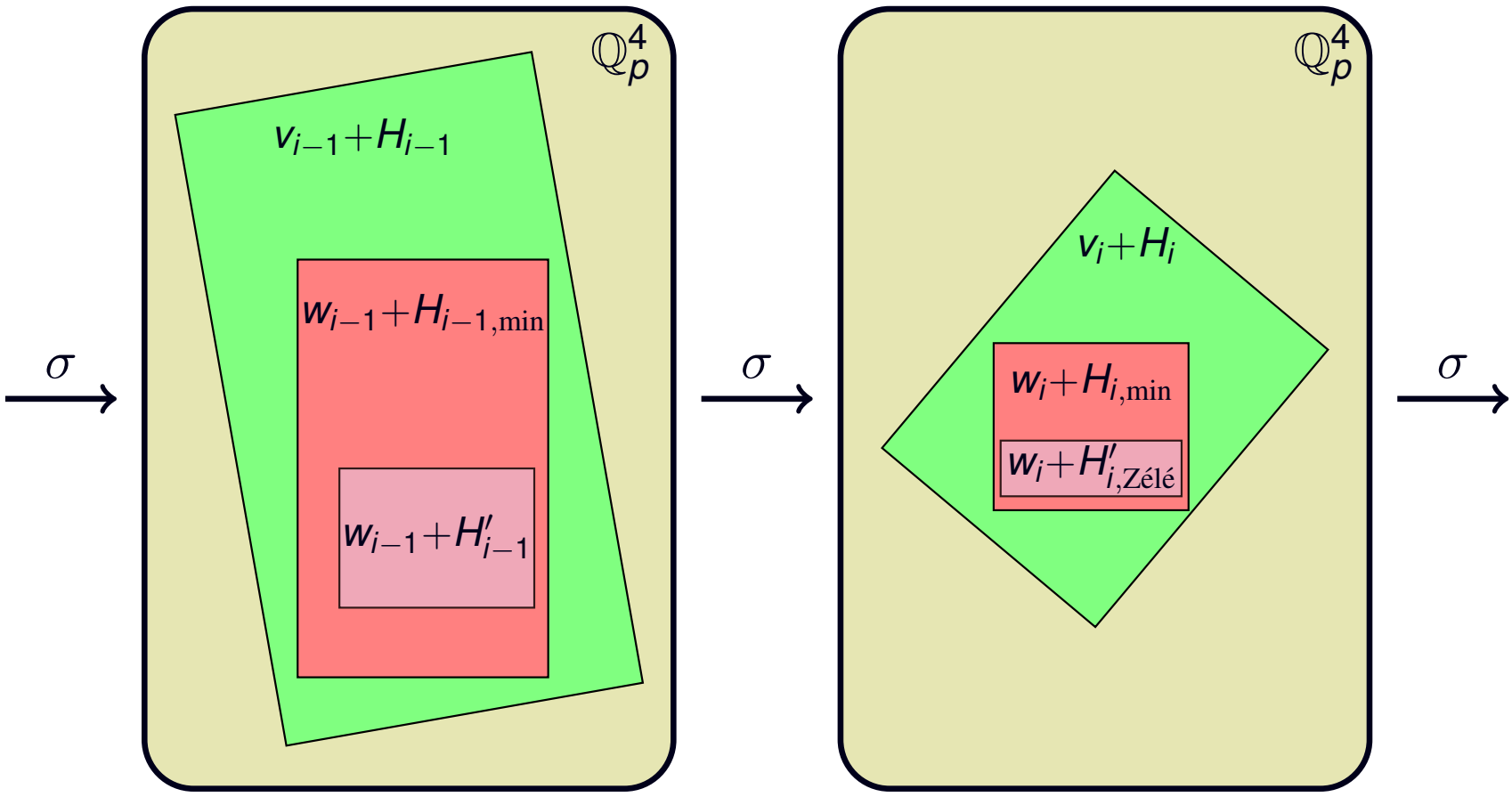
$$p^{N+v(i)}\mathbb{Z}_p^4 \quad \subset \quad d\sigma^i_{(a,b,c,d)}\big(\underbrace{p^N\mathbb{Z}_p^4}_{H}\big) \quad \subset \quad p^N\mathbb{Z}_p^4$$

Exemple : la suite de Somos 4

$$\underbrace{p^{N+v(i)}\mathbb{Z}_p^4}_{H_{i,\min}} \quad \subset \quad d\sigma^i_{(a,b,c,d)}\Big(\underbrace{p^N\mathbb{Z}_p^4}_{H}\Big) \quad \subset \quad \underbrace{p^N\mathbb{Z}_p^4}_{H_{i,\max}}$$

Exemple : la suite de Somos 4

$$\underbrace{p^{N+v(i)}\mathbb{Z}_p^4}_{H_{i,\min}} \subset d\sigma^i_{(a,b,c,d)}\Big(\underbrace{p^N\mathbb{Z}_p^4}_{H}\Big) \subset \underbrace{p^N\mathbb{Z}_p^4}_{H_{i,\max}}$$



Exemple : la suite de Somos 4

$$\underbrace{p^{N+v(i)}\mathbb{Z}_p^4}_{H_{i,\min}} \subset d\sigma^i_{(a,b,c,d)}\Big(\underbrace{p^N\mathbb{Z}_p^4}_{H}\Big) \subset \underbrace{p^N\mathbb{Z}_p^4}_{H_{i,\max}}$$

```
def somos_stabilized(a,b,c,d,n):
    x,y,z,t = a,b,c,d
    for i in 1,2,...,n-4:
        u = (y*t + z*z)/x
        v = val_p(y) + val_p(z) + val_p(t) + val_p(u)
        if v ≥ N: raise PrecisionError
        lift x,y,z,t at precision O(p^(N+v+val_p(x)))
        x,y,z,t = y, z, t, (y*t + z*z)/x
    return t at precision O(p^N)
```

Exemple : la suite de Somos 4

$$\underbrace{p^{N+v(i)}\mathbb{Z}_p^4}_{H_{i,\min}} \subset d\sigma^i_{(a,b,c,d)}\Big(\underbrace{p^N\mathbb{Z}_p^4}_{H}\Big) \subset \underbrace{p^N\mathbb{Z}_p^4}_{H_{i,\max}}$$

```
def somos_stabilized(a,b,c,d,n):
    def nth_term(N):
        x,y,z,t = a(N),b(N),c(N),d(N)
        for i in 1,2,...,n-4:
            u = (y*t + z*z) / x
            v = val_p(y) + val_p(z) + val_p(t) + val_p(u)
            if v ≥ N: raise PrecisionError
            x,y,z,t = y % p^(N+v), z % p^(N+v),
                      t % p^(N+v), u % p^(N+v)
        return t % p^N
    return nth_term
```

Exemple : la suite de Somos 4

$$\underbrace{p^{N+v(i)}\mathbb{Z}_p^4}_{H_{i,\min}} \subset d\sigma^i_{(a,b,c,d)}\Big(\underbrace{p^N\mathbb{Z}_p^4}_{H}\Big) \subset \underbrace{p^N\mathbb{Z}_p^4}_{H_{i,\max}}$$

```
def somos_stabilized(a,b,c,d,n):
    def nth_term(N):
        x,y,z,t = a(N),b(N),c(N),d(N)
        for i in 1,2,...,n-4:
            u = (y*t + z*z) / x
            v = val_p(y) + val_p(z) + val_p(t) + val_p(u)
            if v ≥ N: return nth_term(2*N)
            x,y,z,t = y % p^(N+v), z % p^(N+v),
                      t % p^(N+v), u % p^(N+v)
        return t % p^N
    return nth_term
```

C’est fini, les amis