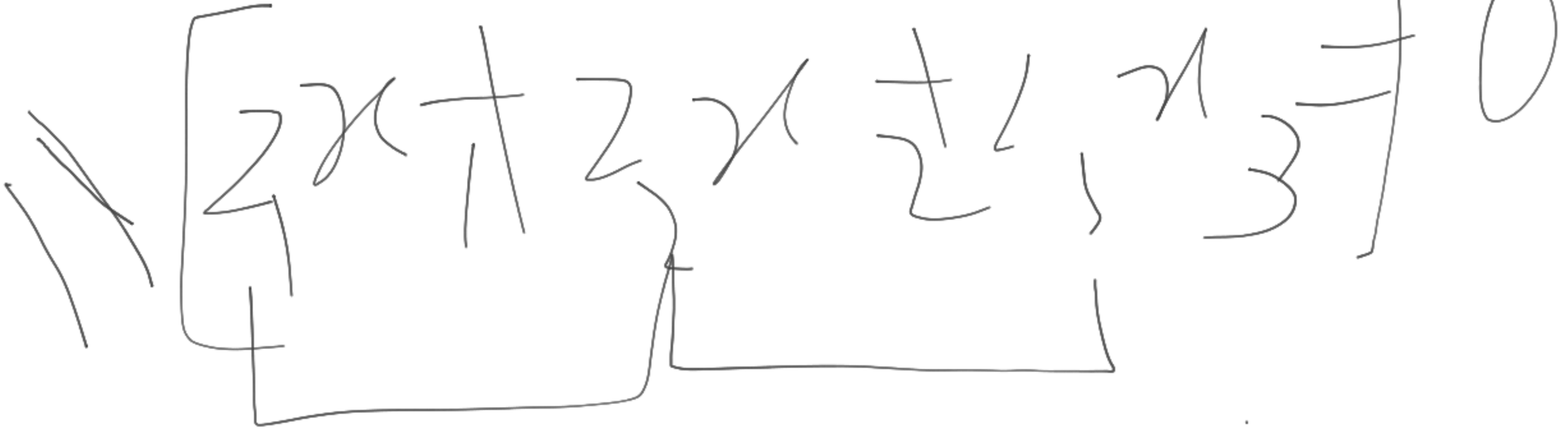
LWE

SIS



[A]

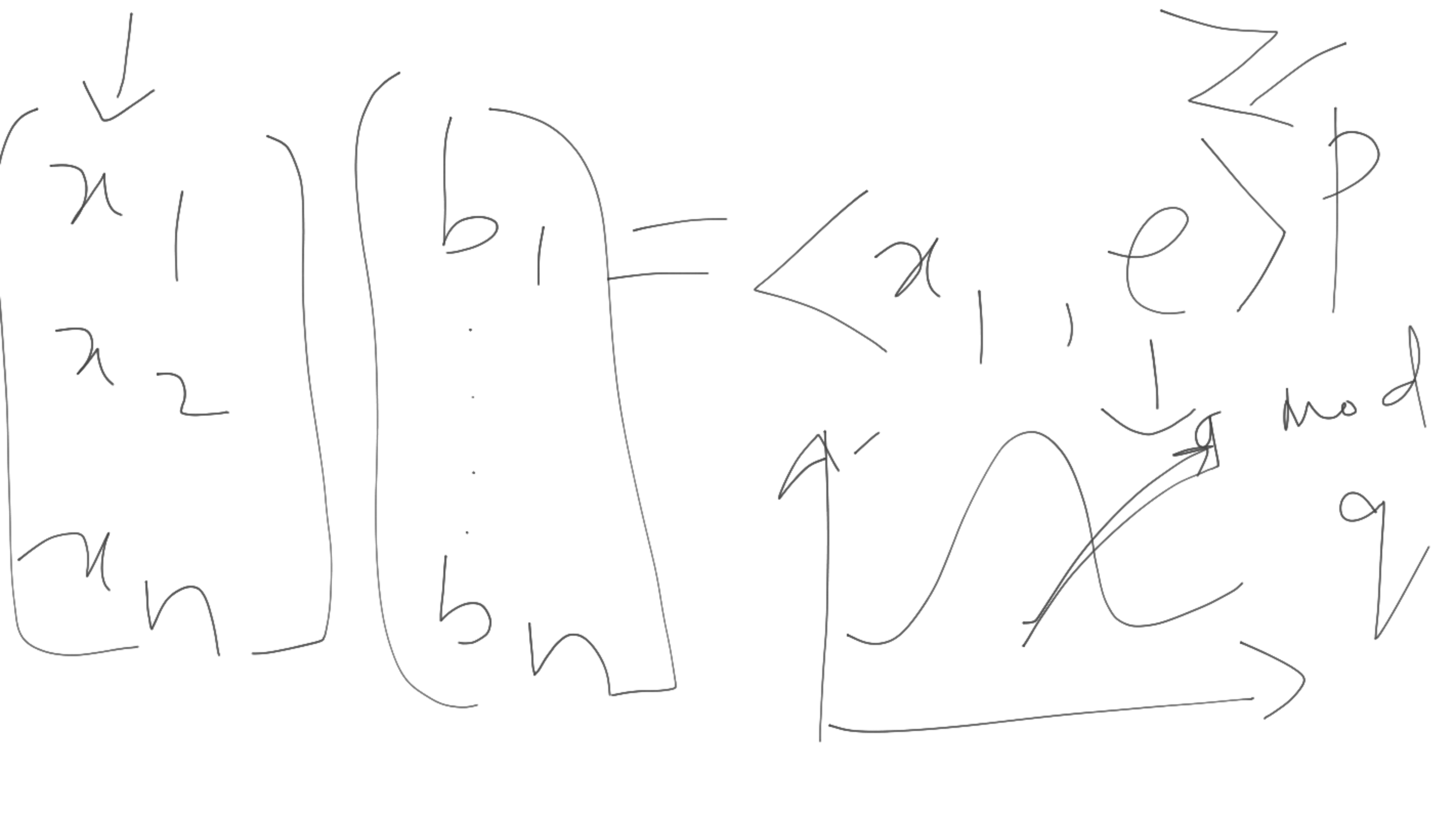
$\bar{z}_1 x_1 + \bar{z}_2 x_2 + \bar{z}_3 x_3 = 0$

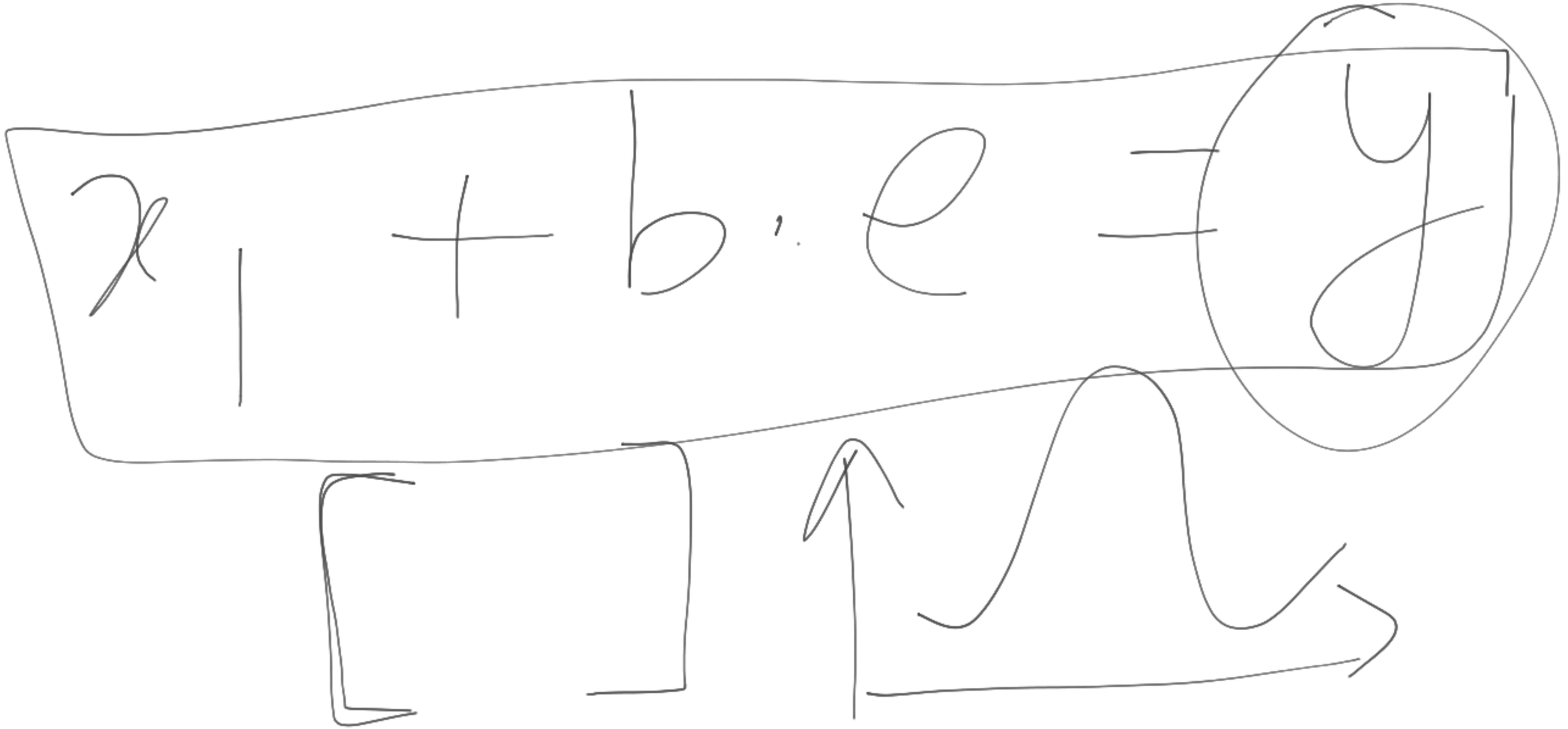
→ $x_1, x_2, x_3 \in \mathbb{Z}_p$

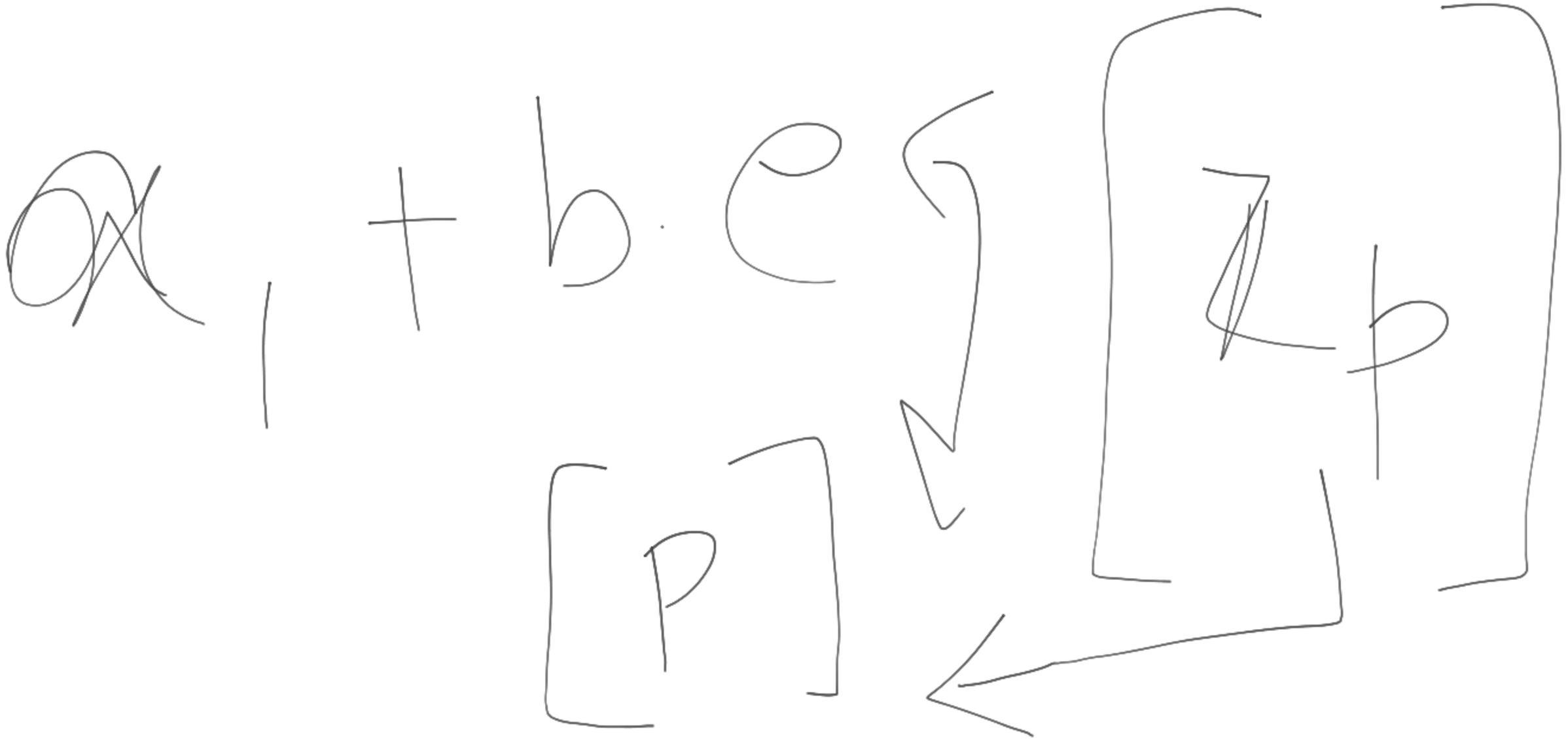
LWE

$x_1, x_2 \ldots x_n$

$b = \langle s, e \rangle$

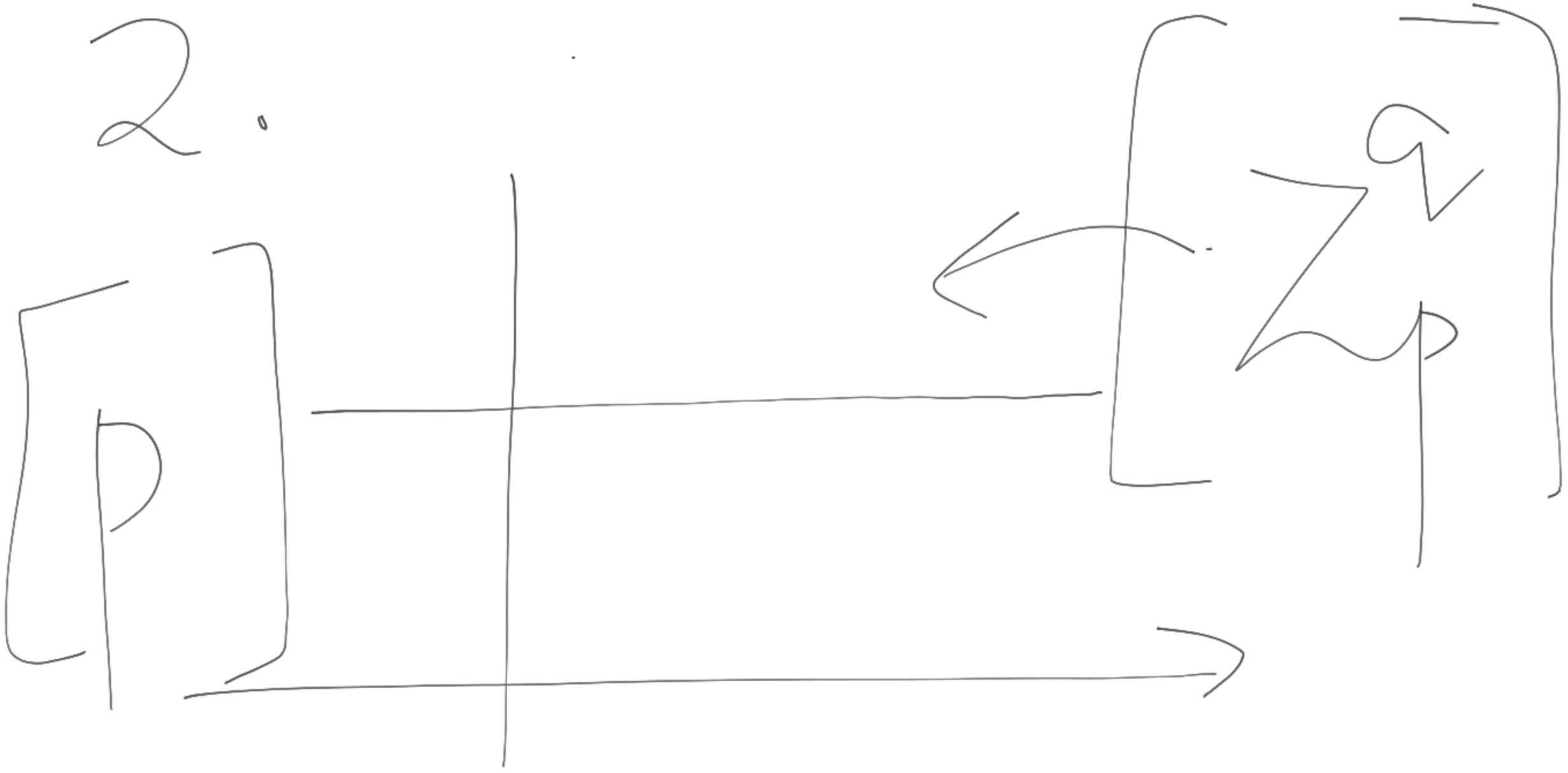



$x_1 + b \cdot e = y$



2 case

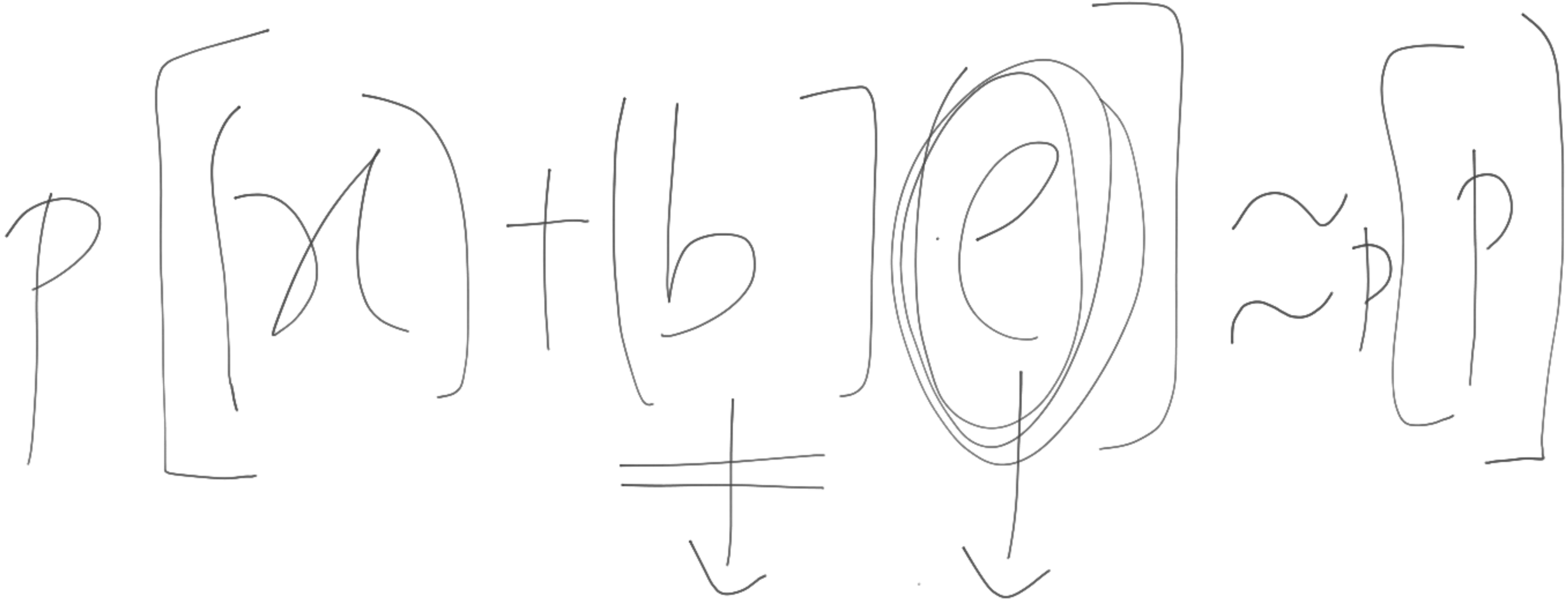
1. $[x] + [b]\vec{e} = [y]$

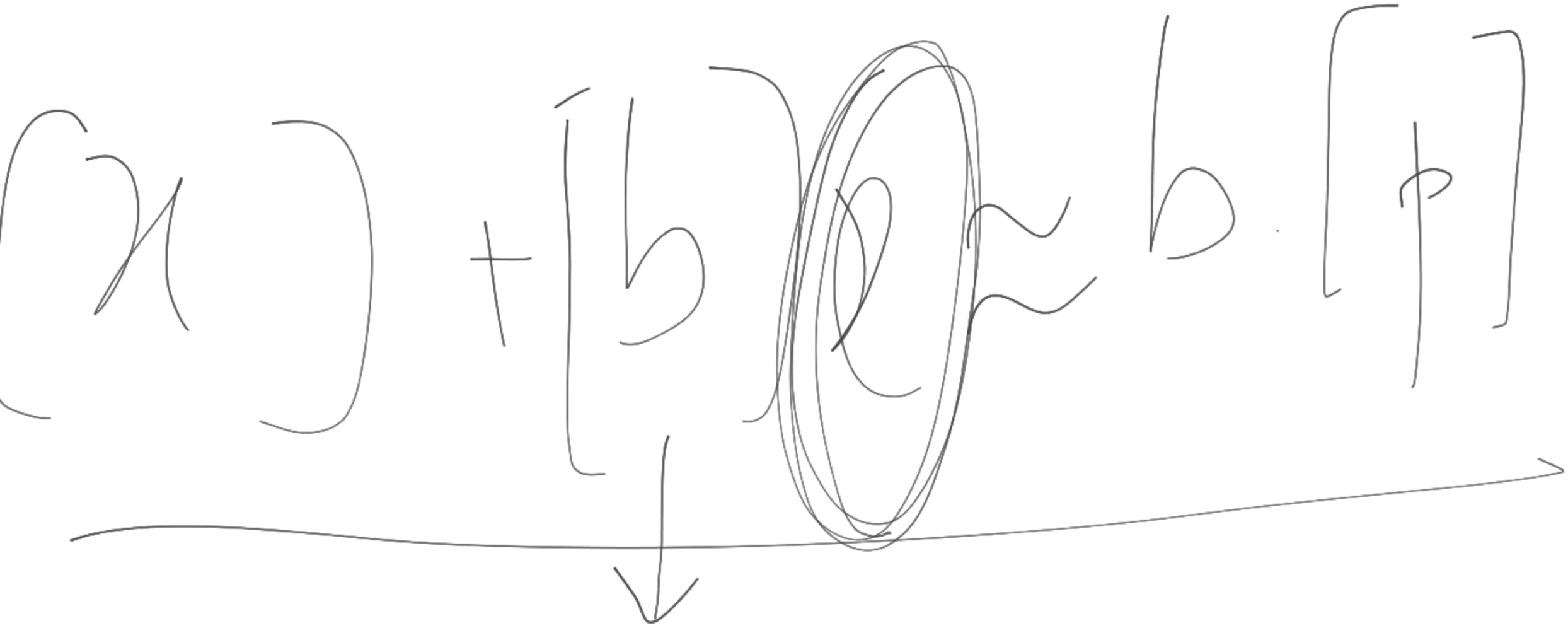

2.

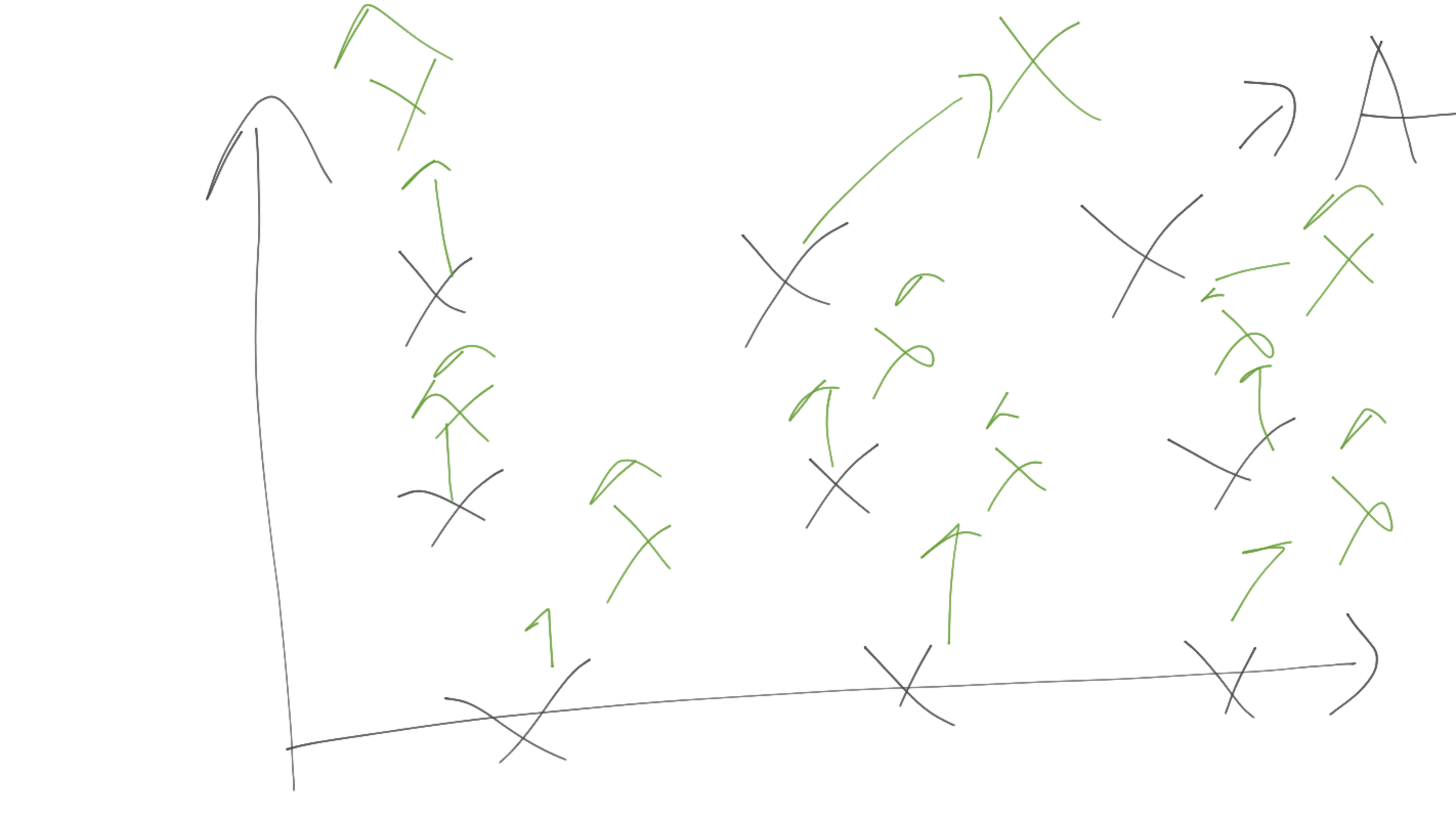
1. Causality →

2. Naturally


10th







$A = [A] \rightarrow$ public

$[A] + [b]e^{-}$