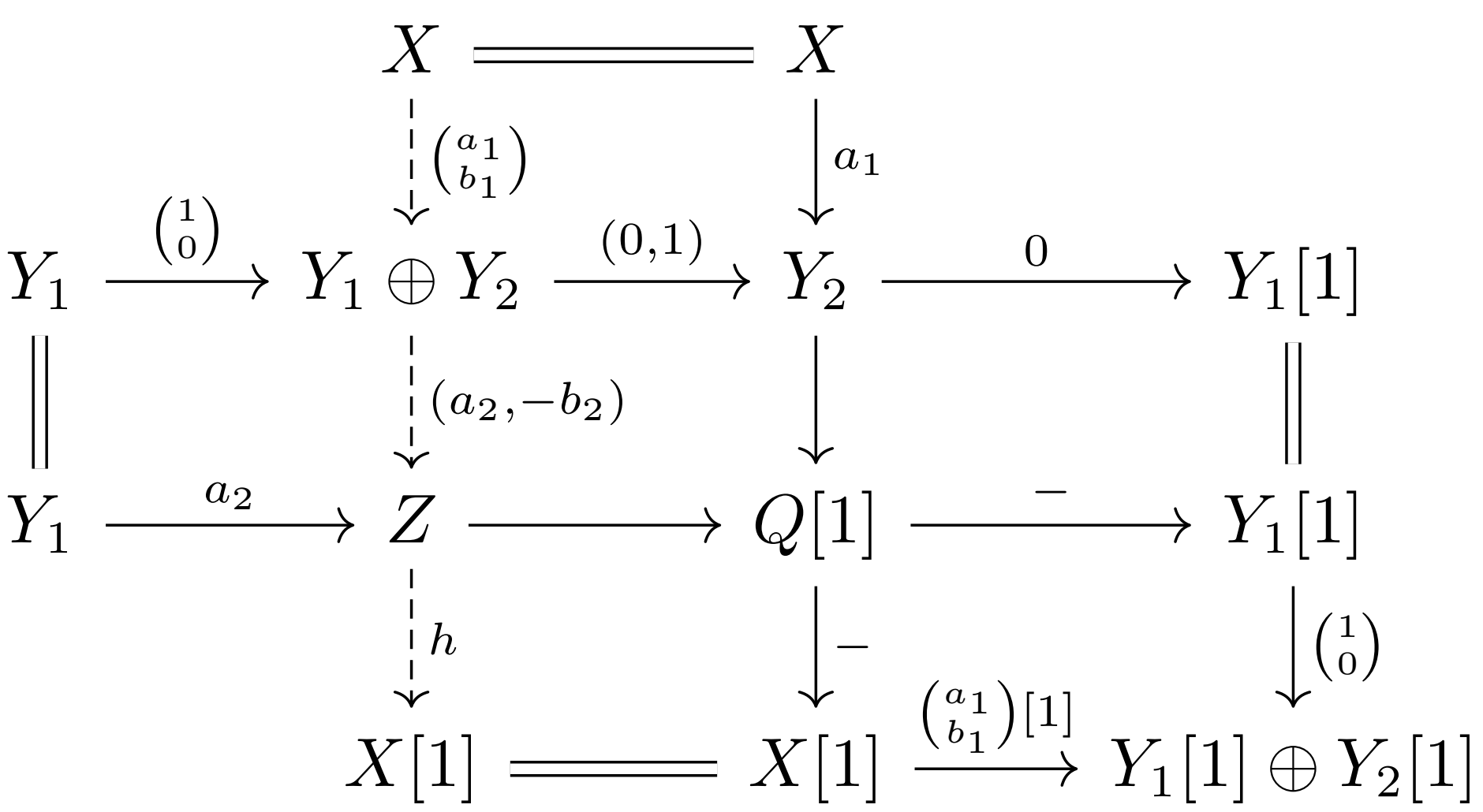
X
X
$\binom{a_1}{b_1}$
a_1
$\binom{1}{0}$
Y_1
$Y_1 \oplus Y_2$
$(0,1)$
Y_2
0
$Y_1[1]$
$(a_2, -b_2)$
Y_1
a_2
Z
$Q[1]$
$-$
$Y_1[1]$
h
$-$
$\binom{1}{0}$
$X[1]$
$X[1]$
$\binom{a_1}{b_1}[1]$
$Y_1[1] \oplus Y_2[1]$