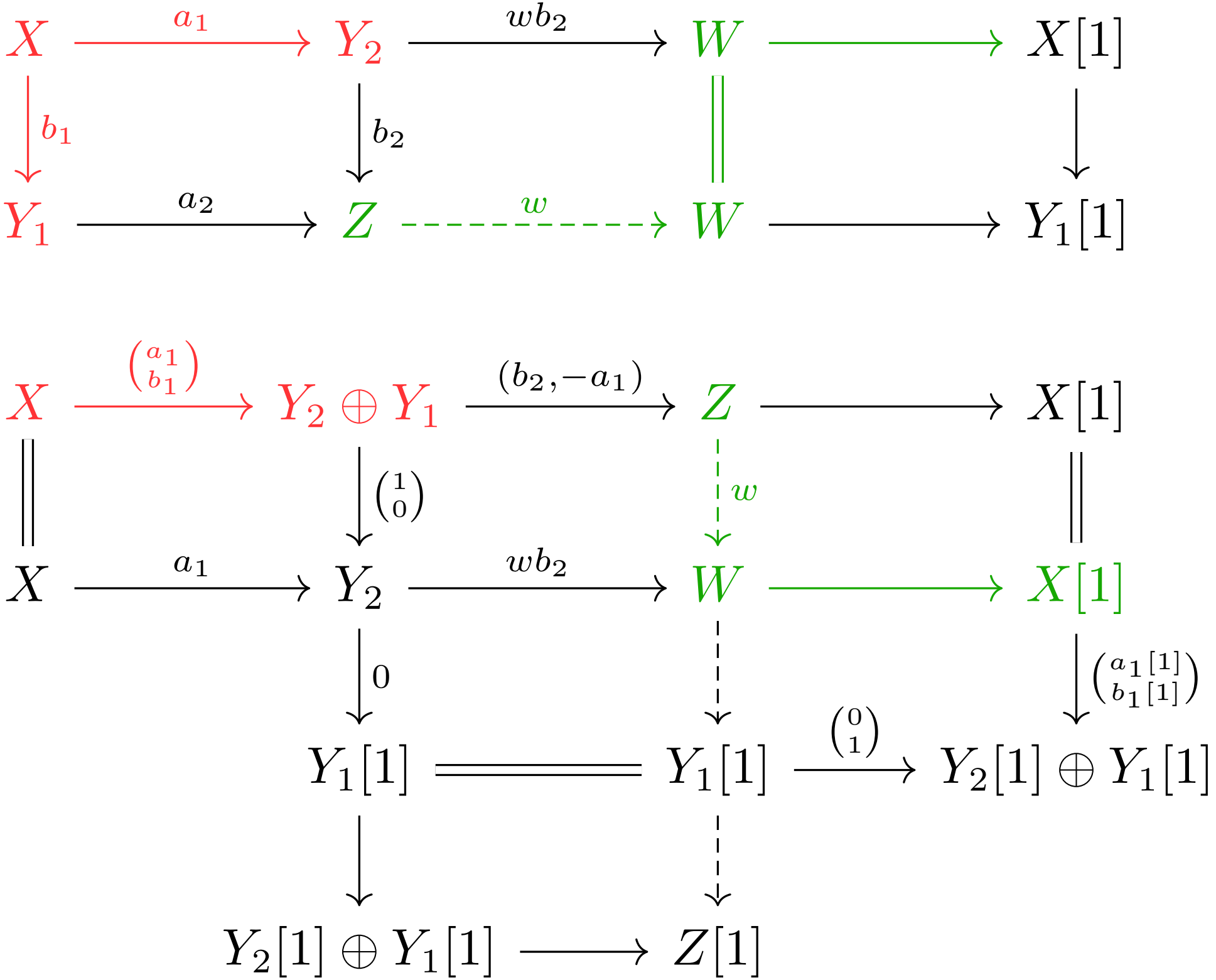
X
a1
Y2
wb2
W
X[1]
b1
b2
Y1
a2
Z
w
W
Y1[1]
X
(a1 b1)
Y2 ⊕ Y1
(b2, −a1)
Z
X[1]
(1 0)
w
X
a1
Y2
wb2
W
X[1]
0
(a1[1] b1[1])
Y1[1]
Y1[1]
(0 1)
Y2[1] ⊕ Y1[1]
Y2[1] ⊕ Y1[1]
Z[1]