$E(g^a, r, M)$ 

 $D(g^r, g^{ar}M, a)$ 

 $=\langle g^r, (g^a)^r M \rangle$ 

 $g^{ar}M$ 

 $(g^r)^a$