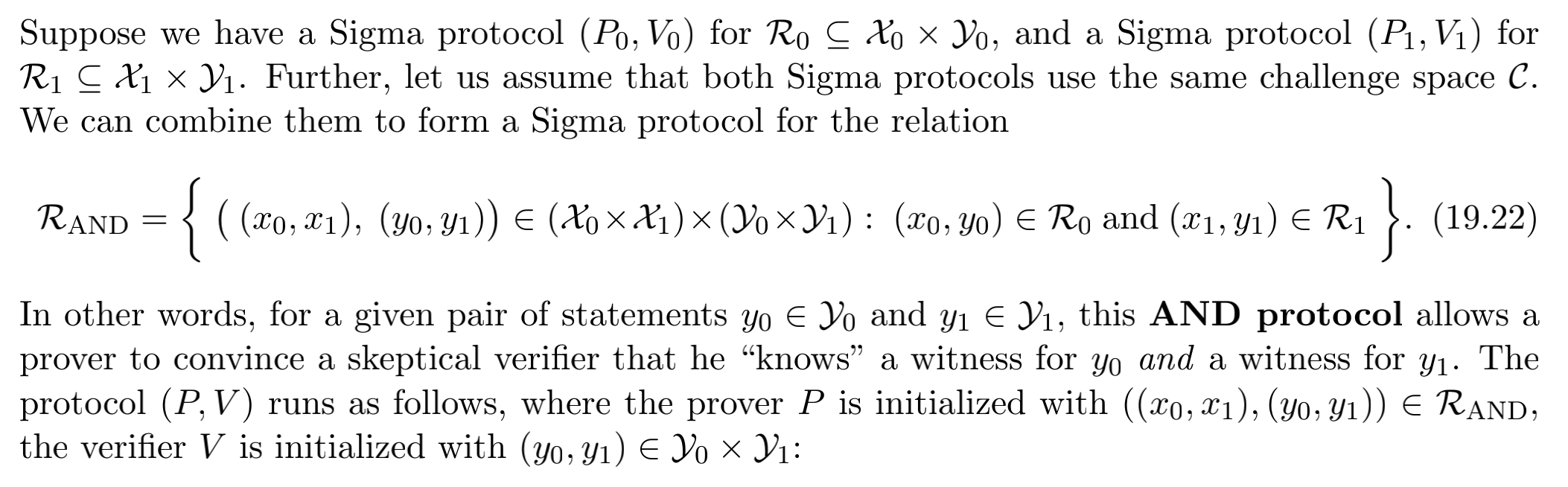
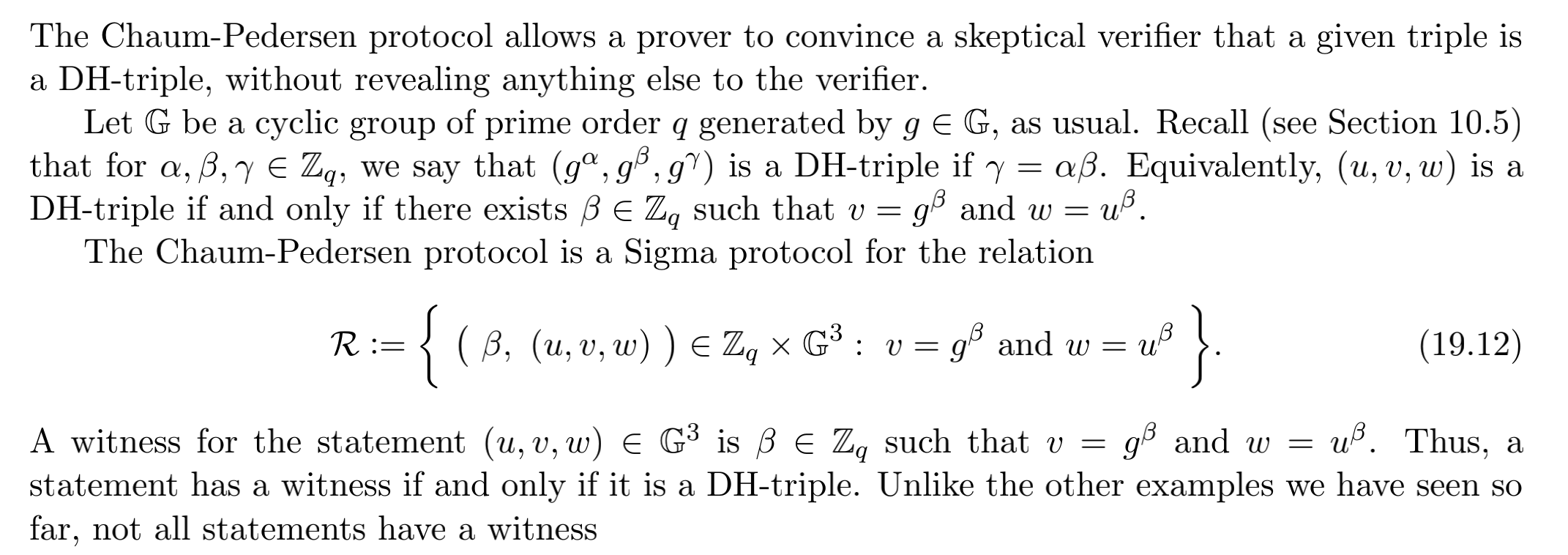
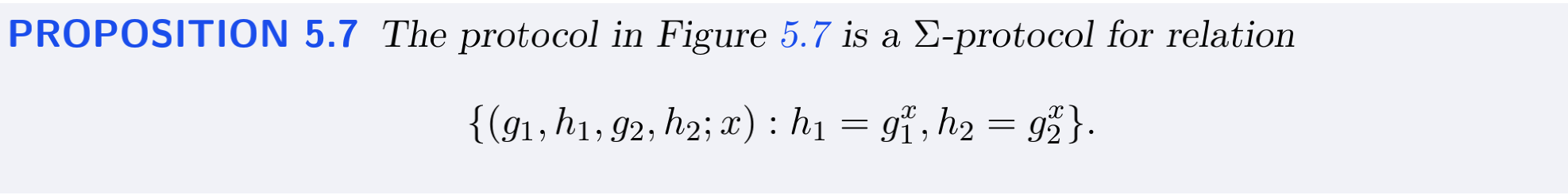
题目1：今天讨论班已经证明OR-construction，能否给出And-construction的构造和证明过程？



题目2：构建sigma协议，能够证明下面的三元组(u ,v, w)是DH-triple。

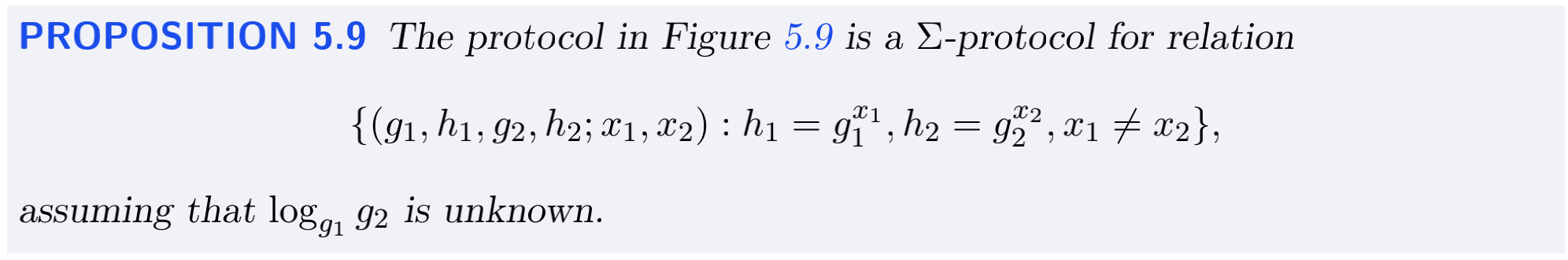


问题3：构建sigma协议，能够证明以下等式成立。



注意(g1,h1,g2,h2)为公开参数，x为私密参数

问题4：构建sigma协议，能够证明以下等式成立。



注意(g1,h1,g2,h2)为公开参数，x1和x2为私密参数