

Lemma: Suppose  $H$  is a subgroup of a group  $G$ . Then,

① the identity element of  $H$  is the same as the identity element of  $G$ .

② If  $a \in H$ , then the inverse of  $a$  in  $H$  is the same as the inverse of  $a$  in  $G$ .

proof: ① Suppose  $e_H$  is the identity of  $H$  and  $e_G$  is the identity of  $G$ . We know that

$$e_H * e_G = e_H = e_H * e_H \quad (*)$$

Suppose  $e_H^{-1}$  is the inverse of  $e_H$  in  $G$ . Then applying  $e_H^{-1}$  to  $(*)$  gives

$$\underbrace{e_H^{-1} * e_H}_{e_G} * e_H = \underbrace{e_H^{-1} * e_H}_{e_H} * e_H$$

So,  $e_G = e_H$ .

② Let  $a \in H$  and  $e$  be the identity of  $G$  (and  $H$ ). Suppose  $a_H^{-1}$  is the inverse of  $a$  in  $H$  and  $a_G^{-1}$  is the inverse of  $a$  in  $G$ . Then,

$$a * a_H^{-1} = e = a * a_G^{-1}$$

$$\text{Thus, } \underbrace{a_H^{-1}}_{a_H^{-1}} = \underbrace{a_H^{-1} * a}_{e} * a_H^{-1} = \underbrace{a_H^{-1} * a}_{e} * a_G^{-1} = a_G^{-1}$$

