Proposition 3.11. *For any subgroup H of a group G, the congruence* mod h *relation* $\underset{H}{\sim}$ *on the elements of G defined by*

$$\forall\, a,\, b \in G, \quad a \underset{H}{\sim} b \Leftrightarrow ab^{-1} \in H$$

is an equivalence relation on the set G, and the equivalence class of $a \in G$ is the right coset Ha.

Proof Let G be a group and H be a subgroup of G.

To show that the congruence mod h relation $\underset{H}{\sim}$ is an equivalence relation on the set G, we need to check that it is reflexive, symmetric and transitive.

(i) Reflexivity Pick $a \in G$. By the identity axiom of H, $1_G \in H$. By the inverse axiom of G, $aa^{-1} = 1_G \in H$. Hence $a \underset{H}{\sim} a$.

(ii) Symmetry Pick $a,\, b \in G$. Suppose that $a \underset{H}{\sim} b$. Then $ab^{-1} \in H$.

To show that $b \underset{H}{\sim} a$, we need to show that $ba^{-1} \in H$.

By the inverse axiom of H, $(ab^{-1})^{-1} \in H$.

By Proposition 1.8,

$$(ab^{-1})^{-1} \underset{\substack{\uparrow \\ \text{by Prop. 1.8 (i)}}}{=} (b^{-1})^{-1} a^{-1} \underset{\substack{\uparrow \\ \text{by Prop. 1.8 (ii)}}}{=} ba^{-1}.$$

Hence, as required, $ba^{-1} \in H$.

(iii) Transitivity Pick $a,\, b,\, c \in G$. Suppose that $a \underset{H}{\sim} b$ and $b \underset{H}{\sim} c$. Then $ab^{-1},\, bc^{-1} \in H$.

To show that $a \underset{H}{\sim} c$, we need to show that $ac^{-1} \in H$.

By the closure axiom of H, $(ab^{-1})(bc^{-1}) \in H$.

Using the associativity, inverse and identity axioms of G gives that

$$(ab^{-1})(bc^{-1}) \underset{\substack{\uparrow \\ \text{by associativity} \\ \text{axiom of } G}}{=} a(b^{-1}(bc^{-1})) \underset{\substack{\uparrow \\ \text{by associativity} \\ \text{axiom of } G}}{=} a((b^{-1}b)c^{-1}) \underset{\substack{\uparrow \\ \text{by inverse} \\ \text{axiom of } G}}{=} a(1_G c^{-1}) \underset{\substack{\uparrow \\ \text{by identity} \\ \text{axiom of } G}}{=} ac^{-1}.$$

Hence, as required, $ac^{-1} \in H$.