

10.5 Lemma: *Let $H \subseteq G$. Right congruence modulo H and left congruence modulo H are equivalence relations on G .*

Proof: We give the proof for right congruence only. We check that it is reflexive, symmetric and transitive.

(i) For all $a \in G$, $a \equiv_l a \pmod{H}$, as this means $aa^{-1} = 1 \in H$. So right congruence is reflexive. Reflexivity of right congruence follows from the fact that $1 \in H$.

(ii) If $a \equiv_r b \pmod{H}$, then $ab^{-1} \in H$, then $(ab^{-1})^{-1} \in H$, hence $ba^{-1} \in H$ and $b \equiv_r a \pmod{H}$. So right congruence is symmetric. Symmetry of right congruence follows from the fact that H is closed under the forming of inverses.

(iii) If $a \equiv_r b \pmod{H}$ and $b \equiv_r c \pmod{H}$, then $ab^{-1} \in H$ and $bc^{-1} \in H$, then $(ab^{-1})(bc^{-1}) \in H$, hence $ac^{-1} \in H$ and $a \equiv_r c \pmod{H}$. So right congruence is transitive. Transitivity of right congruence follows from the fact that H is closed under multiplication.

Hence right congruence is an equivalence relation on G .

According to Theorem 2.5, G is the disjoint union of right congruence classes.

The right congruence class of $a \in G$ is the right coset of a :

$$\begin{aligned}
 [a] &= \{x \in G : x \equiv_r a \pmod{H}\} \\
 &= \{x \in G : xa^{-1} \in H\} \\
 &= \{x \in G : xa^{-1} = h, (\text{where}) h \in H\} \\
 &= \{x \in G : x = ha, (\text{where}) h \in H\} \\
 &= \{ha \in G : h \in H\} \\
 &= Ha.
 \end{aligned}$$

This gives a new proof of Lemma 10.3.

10.6 Lemma: *Let $H \subseteq G$. There are as many distinct right cosets of H in G as there are distinct left cosets of H in G . More precisely, let R be the set of right cosets of H in G and let L be the set of left cosets of H in G . Then R and L have the same cardinality $|R| = |L|$.*