1. Quotient Groups and Homomorphisms

1.1. Cosets and counting

Let $(G, \cdot)$ be a group.

Definition 1.1. Let $H \leq G$ and $a, b \in G$. Define $\cong_r$ over G by

$$a \cong_r b \iff ab^{-1} \in H.$$

Whenever $a \cong_r b$ we say a right is congruent to b module H. Define $\cong_l$ over G by

$$a \cong_l b \iff a^{-1}b \in H.$$

Whenever $a \cong_l b$ we say a is left congruent to b module H.

Remark 1.1.1. If G is Abelian,

$$ab^{-1} \in H \iff a^{-1}b \in H$$

for any $a, b \in G$.

Theorem 1.2. *Let $H \leq G$.*

(i) Right and left congruence module H are both equivalence relations on G.

(ii) The equivalence class of $a \in G$ under right congruence mod H is the set

$$Ha = \{ha \mid h \in H\}$$

(iii) The equivalence class of $a \in G$ under left congruence mod H is the set

$$aH = \{ah \mid h \in H\}$$

(iv) $|Ha| = |H| = |aH|$ for any $a \in G$.

We call aH the left coset of H by a in G, and Ha the a right coset of H by a in G.

Remark 1.2.1. In additive notation (that is, when we are working with an Abelian group) we write $a + H$ instead of aH and $H + a$ instead of Ha. In fact, there is no difference between left and right cosets in this case. (Why $a + H = H + a$ for any $a \in G$?)

Proof. (i)

□

Corollary 1.3. *Let $H \leq G$.*

(i) $G = \bigcup_{a \in G} Ha = \bigcup_{a \in G} aH$

(ii) For all $a, b \in G$ distinct, $aH \cap bH = \emptyset$ and $Ha \cap Hb = \emptyset$.

(iii) For all $a, b \in G$, we have $aH = bH$ if and only if $a^{-1}b \in H$ (or $b - a \in H$ in additive notation) and $Ha = Hb$ if and only if $ab^{-1} \in H$ (or $b - aa \in H$ in additive notation).

(iv) If $\mathcal{R} = \{Ha \mid a \in G\}$ and $\mathcal{L} = \{aH \mid a \in G\}$ then $|\mathcal{R}| = |\mathcal{L}|$.

A special name and notation have been adopted for the number of left (or right) cosets of a subgroup in a group.

Definition 1.4 (Index)**.** The index of a subgroup H in G is the number of distinct left cosets of H in G. This number is denoted by $|G : H|$.

Exercise 1. Prove $|G : H|$ equals the number of distinct right cosets of H in G.

Theorem 1.5. *If K, H, G are groups with $k < H < G$ then*

$$[G : k] = [G : H] \cdot [H : k]$$

If any two of these indices are finite, so is the third.

Proof. □

Corollary 1.6 (Lagrange's theorem)**.** *If $H \leq G$, then $|G| = [G : H]|H|$. In particular, if G is finite, the order of any $a \in G$ divides $|G|$.*

Proof. □

Theorem 1.7. *Let H and K be finite subgroups of a group G. Then*

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Proposition 1.8.

Proof. □

Proposition 1.9.