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 $\cong_l$ 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. Define $\cong_r$ over G by

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

Whenever $a \cong_r b$ we say a is right congruent to b module H.

Remark 1.1.1. If G is Abelian,

$$a - b \in H \iff b - a \in H$$

for any $a, b \in G$. This is not true in general unless G is Abelian.

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

(i) Both $\cong_l$ and $\cong_r$ are equivalence relations on G.

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

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

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

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

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

Proof. Try it yourself (or classwork). □

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 $a \in G$?)

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 $b - a \in H$ 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. Thus it does not matter whether we count left or right cosets.

Definition 1.5. A **complete set of right representatives** of H is a subset S of G consisting of exactly one element from each right coset. In other words, $S \cap Ha$ is a singleton for every $a \in G$.

Define a *complete set of left representatives* in the obvious way. Note that such a set (either left or right) contains exactly one element of H since $H = He$, where e is the identity of G. (What is the cardinality of a complete set of representatives?) Further, if $H = \langle e \rangle$, then $Ha = \{a\}$ for any $a \in G$, and $|G : H| = |H|$, that is, there are as many left (or right) cosets as the number of elements of G.

Theorem 1.6. *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. Let Λ be a complete set of right representatives of H in G. By Corollary 1.3,

$$G = \bigcup_{a \in G} Ha = \bigcup_{a \in \Lambda} Ha.$$

Basically, we are joining all the equivalence classes given by right congruence modulo H, and their union covers G (why?) Similarly, let Ω be a complete set of right representatives of K in H and write

$$H = \bigcup_{b \in \Omega} Kb.$$

Therefore,

$$G = \bigcup_{a \in \Lambda} Ha = \bigcup_{a \in \Lambda} \left(\bigcup_{b \in \Omega} Kb \right) a = \bigcup_{(a,b) \in \Lambda \times \Omega} Kba$$

(If you are not confortable with this, you should review the definition of a union over a multiple indexed family of sets. See here and here (page 35).) Let's now prove that the cosets Kba are mutually disjoint. Suppose $Kba = Kb'a'$. Then $ba = kb'a'$ for some $k \in K$. Since $b, b', k \in H$, have $Ha = Hba = Hkb'a' = Ha'$, whence $a = a'$ because we are working with complete sets of representatives. Thus $b = kb'$. The same reasoning gives $Kb = Kkb' = Kb'$ whence $b = b'$. This proves the cosets Kba are pairwise disjoint. Finally, it follows that $|G : K| = |\Lambda \times \Omega|$ by definition of index, and so

$$|G : K| = |\Lambda||\Omega| = |G : H||H : K|,$$

as desired. The last statement of the theorem is obvious. $\square$

Corollary 1.7 (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. Apply the last theorem with $K = \langle e \rangle$ for the first statement. The second is a special case of the first with $H = \langle a \rangle$. $\square$

If G is a group and H, K are subsets of G, we denote by HK the set $\{ab \mid a \in H, b \in K\}$. Note that a right or left coset of a subgroup is a special case of this construction.

Remark 1.7.1. Careful! If H, K are subgroups, HK may not be a subgroup.

Theorem 1.8. *Let H and K be finite subgroups of a group G. Then*

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

Proof. Note $C = H \cap K$ is a subgroup of K of index $n = |K|/|H \cap K|$ and K is the disjoint union of right cosets $Ck_1 \cup Ck_2 \cup \ldots \cup Ck_n$ for some $k_i \in K$. Since $HC = H$, this implies that HK is the union of the disjoint sets $Hk_1 \cup Hk_2 \cup \cdots \cup Hk_n$. Therefore, $|HK| = |H| \cdot n = |H||K|/|H \cap K|$. $\square$

Proposition 1.9. If H and K are subgroups of a group G, then $[H : H \cap K] \leq [G : K]$. If $[G : K]$ is finite, then $[H : H \cap K] = [G : K]$ if and only if $G = HK$.

$$\begin{tikzcd}[column sep=small]
& G \arrow[dl, dash] \arrow[dr, dash] & \\
H \arrow[dr, dash] & & K \arrow[dl, dash] \\
& H \cap G &
\end{tikzcd}$$

Proof. Let A be the set of all right cosets of $H \cap K$ in H and B the set of all right cosets of K in G. The map $\varphi : A \to B$ given by $(H \cap K)h \mapsto Kh$, with $h \in H$, is well defined since $(H \cap K)h' = (H \cap K)h$ implies $h'h^{-1} \in H \cap K \subset K$ and hence $Kh' = Kh$. Complete the proof by following these simple steps:

(i) Show that φ is injective. Then $|H : H \cap K| = |A| \leq |B| = |G : K|$.

(ii) If $|G : K|$ is finite, then show that $|H : H \cap K| = |G : K|$ if and only if φ is surjective.

(iii) φ is surjective if and only if $G = KH$.

(Hint: note that for $h \in H$ and $k \in K$, we have $Kkh = Kh$ since $(kh)h^{-1} = k \in K$.) Conclude. $\square$

Proposition 1.9. *Let H and K be subgroups of G with finite index of a group G. Then $|G : H \cap K|$ is finite and $|G : H \cap K| \leq |G : H||G : K|$. Furthermore, $|G : H \cap K| = |G : H||G : K|$ if $G = HK$.*

Proof. Classwork. $\square$