Cosets

Definition

Let $H \leq G$. The *left* and *right* relations on G are defined as follows:

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

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

Theorem

$\sim_L$ and $\sim_R$ are equivalence relations.

Proof

R: Assume $a \in G$
- $a^{-1} \in G$
- $e \in H$
- $a^{-1}a = e \in H$
- $\therefore a \sim_L a$

S: Assume $a \sim_L b$
- $a^{-1}b \in H$
- $(a^{-1}b)^{-1} \in H$
- $b^{-1}a \in H$
- $\therefore b \sim_L a$

T: Assume $a \sim_L b$ and $b \sim_L c$
- $a^{-1}b \in H$ and $b^{-1}c \in H$
- $(a^{-1}b)(b^{-1}c) \in H$
- $a^{-1}c \in H$
- $\therefore a \sim_L c$

R: Assume $a \in G$
- $a^{-1} \in G$
- $e \in H$
- $aa^{-1} = e \in H$
- $\therefore a \sim_R a$

S: Assume $a \sim_R b$
- $ba^{-1} \in H$
- $(ba^{-1})^{-1} \in H$
- $ab^{-1} \in H$
- $\therefore b \sim_R a$

T: Assume $a \sim_R b$ and $b \sim_R c$
- $ba^{-1} \in H$ and $cb^{-1} \in H$
- $(cb^{-1})(ba^{-1}) \in H$
- $ca^{-1} \in H$
- $\therefore a \sim_R c$

Assume $a \in G$
Assume $g \in G, a \sim_L g$
$a^{-1}g \in H$
$\exists\, h \in H, a^{-1}g = h$
$g = ah$

Assume $a \in G$
Assume $g \in G, a \sim_R g$
$ga^{-1} \in H$
$\exists\, h \in H, ga^{-1} = h$
$g = ha$

Definition

Let $H \leq G$ and $a \in G$:

$aH = \{ah \mid h \in H\}$ is called the *left coset* of H containing a

$Ha = \{ha \mid h \in H\}$ is called the *right coset* of H containing a

Note that if G is abelian then $aH = Ha$.

Theorem

Let $H \leq G$ and $a \in G$:

$$|aH| = |Ha| = |H|$$

Proof

Let $\phi : H \to aH$ be defined by $\phi(h) = ah$

Assume $\phi(h_1) = \phi(h_2)$
$ah_1 = ah_2$
$h_1 = h_2$
$\therefore \phi$ is one-to-one.

Assume $h' \in aH$
Let $h = a^{-1}h'$
$a \sim_L h'$, so $h \in H$
$\phi(h) = ah = a(a^{-1}h') = h'$
$\therefore \phi$ is onto

$\therefore \phi$ is a bijection and $|H| = |aH|$

Now let $\phi : H \to Ha$ be defined by $\phi(h) = ha$

Assume $\phi(h_1) = \phi(h_2)$
$h_1a = h_2a$
$h_1 = h_2$
$\therefore \phi$ is one-to-one.

Assume $h' \in Ha$
Let $h = h'a^{-1}$
$a \sim_R h'$, so $h \in H$
$\phi(h) = ha = (h'a^{-1})a = h'$
$\therefore \phi$ is onto

$\therefore \phi$ is a bijection and $|H| = |Ha|$

So if $H \leq G$, then aH $(\sim_L)$ and Ha $(\sim_R)$ partition G into equivalence classes of order $|H|$:

Theorem: Lagrange

Let H be the subgroup of a finite group G:

$$|H| \text{ divides } |G|$$

Proof

Let $|H| = m$ and $|G| = n$
Every coset of H has n elements
The cosets are the equivalence classes of a relation that partition G
Assume there are r such equivalence classes
$n = rm$
$\therefore m \mid n$

Definition

Let $H \leq G$. The *index* of H in G, denoted $(G : H)$, is the number of left cosets of H in G:

$$(G : H) = \frac{|G|}{|H|}$$

When determining all of the left (right) cosets of G:

1). $(G:H) = \frac{|G|}{|H|}$

2). $a, b \in G$ are in the same coset if $a \sim_L b$ ($a \sim_R b$)

Example

$S_3 = \{(), (12), (13), (23), (123), (132)\}$

Let $H = \{(), (23)\}$

$(S_3 : H) = \frac{6}{2} = 3$

$(12) \notin H$
$(12)^{-1}(13) = (12)(13) = (132) \notin H$
$(12)^{-1}(123) = (12)(123) = (23) \in H$

$()H = \{(), (23)\}$
$(12)H = \{(12), (123)\}$
(13)H={(13),(132)}

$()H = (23)H$
$(12)H = (123)H$
$(13)H = (132)H$

Theorem

Every group of prime order is cyclic.

Proof

Let $|G| = p$, where p is prime
Let $a \in G, a \neq e$
$\langle a \rangle \leq G$ and $|a| \geq 2$
By Lagrange, $|a|$ divides $|G| = p$
But p is prime
So $|a| = p$ and thus $\langle a \rangle = G$
$\therefore G$ is cyclic

Theorem

Let H, K, G be finite groups such that $K \leq H \leq G$:

$$(G:K) = (G:H)(H:K)$$

Proof

$(G:H)(H:K) = \left(\frac{|G|}{|H|}\right)\left(\frac{|H|}{|K|}\right) = \frac{|G|}{|K|} = (G:K)$