MTH 339

Cosets and Lagrange's Theorem

Def Coset of H in G

Let G be a group and H be a nonempty subset of G.

For any $a \in G$, the set $aH := \{ah \mid h \in H\}$ is called the left coset of H in G containing a. $Ha := \{ha \mid h \in H\}$ is called the right coset of H in G containing a.

We also define $aHa^{-1} = \{aha^{-1} \mid h \in H\}$.

a is called the coset representative,

$|aH|$ is the number of elements in aH.

Example: $G = S_3$, $H = \{(1), (13)\}$

Remember: S_3 is the set of all one-to-one functions from $\{1,2,3\}$ to itself, and we use cycle notation

(1) is simply the identity $\begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}$

(13) is $\begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$

Clearly $(1)H = H$

$(12)H = \{(12), (12)(13)\}$

$= \{(12), (132)\}$

$(12)(13)$ is $\begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} = (1\ 3\ 2)$

(Apply first $1 \to 3 \to 1$, so swap 1 and 3, then swap 1 and 2)

Example: Let $H = \{0, 3, 6\}$ in $\mathbb{Z}_9$ under addition. We use the notation $a+H$ instead of aH.

$$0+H = \{0, 3, 6\} = 3+H = 6+H$$
$$1+H = \{1, 4, 7\} = 4+H = 7+H$$
$$2+H = \{2, 5, 8\} = 5+H = 8+H$$

Remark: We observe that cosets are usually not subgroups. Usually $aH = bH$ does not imply necessarily $a = b$.

Lemma: Properties of Cosets

Let H be a subgroup of G, and $a, b \in G$

1./ $a \in aH$

2./ $aH = H$ if and only if $a \in H$

3./ $(ab)H = a(bH)$ and $H(ab) = (Ha)b$

4./ $aH = bH$ if and only if $a \in bH$

5./ $aH = bH$ or $aH \cap bH = \phi$

6./ $aH = bH$ if and only if $a^{-1}b \in H$

7./ $|aH| = |bH|$

8./ $aH = Ha$ if and only if $H = aHa^{-1}$

9./ aH is a subgroup of G if and only if $a \in H$.

Proof:

1./ $a = ae \in H$.

2./ (Do now)

3./ follows from $(ab)h = a(bh)$
and $h(ab) = (ha)b$

4./ If $aH = bH$, then $ae = a \in bH$.
Conversely, if $a \in bH$, we have
$a = bh$, so $aH = (bh)H = b(hH)$
$= bH$

5./ This follows from 4./:
If $c \in aH \cap bH$, we have $cH = aH$
and $cH = bH$, so $aH = bH$.

6./ Clearly, $aH = bH \iff H = a^{-1}bH$, then the result follows from property 2.

7./ To prove $|aH| = |bH|$, we need to find a one-to-one mapping from aH onto bH. Obviously $ah \to bh$ maps aH onto bH. That it is one-to-one follows directly from the cancellation property.

8./ We know that $aH = Ha$ if and only if $(aH)a^{-1} = (Ha)a^{-1} \cdot H(aa^{-1}) = H$, hence if and only if $aHa^{-1} = H$.

9./ If aH is a subgroup, then it contains the identity e. Thus $aH \cap eH \neq \phi$ and, by property 5, we have $aH = eH = H$. Thus, by property 2, we have $a \in H$. Conversely, if $a \in H$, by property 2, we have $aH = H$.

Note that we might view the cosets of H as partitioning of G into equivalence classes under the equivalence relation $a \sim b$ if $aH = bH$.

Example: If G is $\mathbb{R}^3$ and H is a plane through the origin, the coset $(a,b,c) + H$ is the plane passing through the point (a,b,c) and parallel to H.

Lagrange's Theorem

If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$. Moreover, the number of distinct left (right) cosets of H in G is $|G| / |H|$.

Proof: Let $a_1H, a_2H, \ldots, a_rH$ denote the distinct left cosets of H in G.

Then, for any $a \in G$, we have $aH = a_iH$ for some i. We know $a \in aH$, so each element of G belongs to some coset.

$$G = a_1H \cup \ldots \cup a_rH$$

We know that this union is disjoint.

$$|G| = |a_1H| + \cdots + |a_rH|.$$

Finally, since $|a_iH| = |H|$, we have

$$|G| = r|H|.$$

□

Note, we call r the index of a subgroup H, and we write $r = |G:H|$.

$$|G:H| = |G| / |H|$$

1/ **Corollary:** In a finite group, the order of each element divides the order of the group.

2/ **Corollary:** Groups of prime order are cyclic. Every group of prime order is isomorphic to $\mathbb{Z}_p$.

3/ **Corollary:** Let G be a finite group, $a \in G$. Then $a^{|G|} = e$.

Proof: 1./ We know that the order of an element equals the order of the subgroup generated by this element.

2./ Suppose G has prime order and let $a \in G$, $a \neq e$. Then $|\langle a \rangle|$ divides ?, so $|\langle a \rangle| = |G|$, hence $\langle a \rangle = G$.

Theorem: Fermat's Little Theorem

For every integer a and every prime p, we have $a^p \bmod p = a \bmod p$.

Proof: Division algorithm: $a = pm + r$, where $0 \leq r < p$. Thus $a \bmod p = r \bmod p$.
Therefore, we need to show $r^p \bmod p = r$.
If $r = 0$, this is trivial, so we assume $r \in \mathcal{U}(p)$. Recall: $\mathcal{U}(p) = \{1, 2, \ldots, p-1\}$ under multiplication modulo p.
Then (see above) $r^{p-1} \bmod p = 1$
$\Rightarrow r^p \bmod p = r$

□

Remark: This can be used to test for prime numbers.

Is $z = 2^{257} - 1$ prime?

MTH 339

10/10

If p is prime, we know that $10^p \bmod p = 10 \bmod p$, so $10^{p+1} \bmod p = 100 \bmod p$.

It is easy to compute

$10^{p+1} \bmod p = 10^{2^{257}} \bmod p$ in a few seconds. The result was not 100, so p is not prime ($\rightarrow$ code).

MTH 339 Do Now

1./ Prove $aH = H$ if and only if $a \in H$ (H is a subgroup of G, $a \in G$).

2./ Let $H = \{0, \pm 3, \pm 6, \pm 9, \ldots\}$. Find all the left cosets of H in $\mathbb{Z}$.

3./ Compute $5^{15} \bmod 7$ and $7^{13} \bmod 11$.

MTH 339 - HW

1./ If H is a subgroup of $\mathbb{Z}$ and $\langle 3 \rangle \subseteq H$, prove that $H = \langle 3 \rangle$ or $H = \mathbb{Z}$.

2./ If H and K are subgroups of G and g belongs to G, show that $g(H \cap K) = gH \cap gK$

3./ Let G be a group of order 60. What are the possible orders for the subgroups of G.

4./ Let G be a group with $|G| = pq$ where p and q are prime. Prove that every proper subgroup is cyclic.

5./ Suppose that G is an Abelian group with an odd number of elements. Show that the product of all elements is the identity.