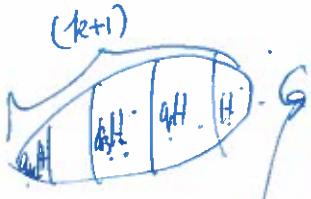


Chapter 7 Cosets and Lagrange's Theorem

Definition Let G be a group and $H \leq G$. For $a \in G$ define the left coset of H containing a by $aH = \{ah : h \in H\}$ and the right coset of H containing by $Ha = \{ha : h \in H\}$.

$|G| = n$
$|H| = k$
There will be $m = \frac{n}{k}$ cosets.

Theorem 7.1 [LaGrange's Theoerem and other properties of cosets] Let G be a group, and $H \leq G$. Define a relation on R on G by $(a, b) \in R$ if $a^{-1}b \in H$. Then R is an equivalence relation so that the left cosets are equivalence classes.

(a) We have $aH = bH$ if and only if $a^{-1}b \in H$.

(b) The group G is a union of disjoint left cosets of H.

(c) The map $ah \mapsto bh$ is a bijection between two cosets aH and bH.

(d) If G is finite, then it is a disjoint union of m left cosets of H with $m = |G|/|H|$.

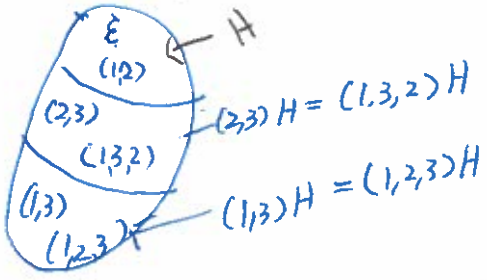
$(2,3)(1,2) = (1,3,2)$.

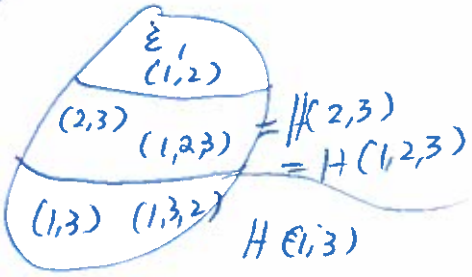
Example S_3 $G = S_3$, $H = \{\varepsilon, (1,2)\}$

$(2,3)H = \{(2,3), (1,2,3)\}$

$H(2,3) = \{(2,3), (1,2,3)\}$

$(1,2)(2,3) = (1,3,2)$





Proof: Define R on G by $(a,b) \in R$ if $a^{-1}b \in H$.

Reflexive: For every $a \in G$, $a^{-1}a = e \in H$, $\therefore (a,a) \in R$

Symmetric: Suppose $(a,b) \in R$, i.e., $a^{-1}b \in H$; $(a^{-1}b)^{-1} \in H$ $\therefore b^{-1}a \in H$, $\therefore (b,a) \in R$

Transitive: Suppose $(a,b), (b,c) \in R$.

Then $a^{-1}b \in H$, $b^{-1}c \in H$, $\therefore (a^{-1}b)(b^{-1}c) \in H$ $\therefore (a,c) \in R$

$a^{-1}c$

$\therefore$ R is an equivalence relation on G.

(a) Let $a \in G$. The equivalence class

$$[a] = \{x \in G : (a,x) \in R\}$$
$$= \{x \in G : a^{-1}x \in H\}$$
$$= \{x \in G : a^{-1}x = h \text{ for some } h \in H\}$$
$$= \{x \in G : x = ah, h \in H\} = \{ah : h \in H\}$$

Example:

$G = \mathbb{Z}$. infinite;

$H = \{\text{even integer}\}$

$H, \ 1+H$

$\langle 1 \rangle = \mathbb{Z}$

1 coset

For $H = \langle k \rangle = k\mathbb{Z}$

$0 + \langle k \rangle = \bar{0}$

$1 + \langle k \rangle = \bar{1}$

$\vdots$

$k-1 + \langle k \rangle = \overline{k-1}$

$\in (\mathbb{Z}_{/k\mathbb{Z}})$

k cosets

$\langle 0 \rangle = H$ has infinitely many cosets

Find — There are finitely many cosets.

Example.

G - infinite

$H \leq G$

Infinitely many cosets of H

$G = \{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{R}) : ad - bc \neq 0 \}$

$H = \{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{R}) : ad - bc = 1 \}$.

For every $a \in \mathbb{R}^*$,

$\begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} H = \{ A \in M_2(\mathbb{R}) : \det(A) = a \}$

$AH = BH \iff A^{-1}B \in H \iff \det(A) = \det(B)$.

So $G = \bigcup_{a \in \mathbb{R}^*} \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} H$.

Lagrange Theorem: Order of a subgroup divides

Notation and Terminology The number of cosets of the subgroup H in G is called the index of H in G, and denoted by $|G : H|$. If G is finite, it is equal to $|G|/|H|$.

Corollary Let G be a finite group. $=$ no. of cosets.

1. If $a \in G$, then $|a|$ is a factor of $|G|$ so that $a^{|G|} = e$.
2. If G has prime order than G is cyclic.

$\Rightarrow$ $|H|$ is a factor of $|G|$.

$|a| = |\langle a \rangle|$ is a factor of $|G|$

$\Downarrow$

$a^{|G|} = e$

Corollary [Fermat's Little Theorem] If $a \in \mathbb{Z}$ and p is a prime, then $a^p - a$ is divisible by p. More generally, if $k \in \mathbb{Z}_n$, then $k^{\phi(n)} = 1$ if $\gcd(k, n) = 1$, i.e., $k \in U(n)$.

Lagrange Theorem: Let $|G| = n$, $H \leq G$, $|H| = m$, then $m \mid n$

If $|G| = p$, then for any $a \in G$, $a \neq e$.

we have $|a| = p$. $G = \langle a \rangle$.

Proof. In $\mathbb{Z}_p$, if $[a] = [0]$, then $[0]^p \equiv [0]$ in $\mathbb{Z}_p$

$\therefore$ $a^p - a$ is divisible by p

If $[a] = [0]$

If $[a] \neq [0]$ in $\mathbb{Z}_p$,

then $[a^{p-1}] = [a]^{p-1} = [1]$ in $\mathcal{U}(p)$

$\therefore$ $[a^p] = [a]$.

$\therefore$ $a^p - a$ is divisible by p.

For general n, $\mathcal{U}(n) = \{\bar{k} \in \mathbb{Z}_n : \gcd(k, n) = 1\}$ is a group of order $\varphi(n)$ elements.

$\therefore$ For any $\bar{k} \in \mathcal{U}(n)$, $\bar{k}^{\varphi(n)} = \bar{1}$

Example. $13^{\varphi(n)} = 1$ in $\mathbb{Z}_n$ if n not divisible by 13

Remarks

1. The converse of Lagrange's Theorem is false. Example 5 in p.149. The group A_4 has order 12, but there is no subgroup of order 6.
2. One may consider the right cosets Ha so that $Ha = Hb$ if and only if $ab^{-1} \in H$, G is a partition of the right cosets.
3. Left and right cosets are different in general.
4. A subgroup H in G satisfies $aH = Ha$ for all $a \in G$ if and only if $aHa^{-1} = H$ for all $a \in G$. Such a subgroup is called a normal subgroup of G.

p.144

Idea of proof. If $H \leq A_4$ with $|H|=6$, then H will contains all order 3 elements $(1,2,3)$ & 8 elements

Question If $|G|=12$, can I always find $H \leq G$ with $|H|=6$?

$Ha = Hb \iff (Ha)b^{-1} = (Hb)b^{-1} = H \Rightarrow \{h_1, \dots h_m\}$

$\Rightarrow Hab^{-1} = H$

$\Rightarrow \{eab^{-1}, h_1 ab^{-1}, \dots h_m ab^{-1}\} = H$

$aH = bH \iff a^{-1}(aH) = a^{-1}bH = \{a^{-1}be, a^{-1}bh, \dots\}$

$= H$

Remark: If G is Abelian then for any $H \leq G$, $aH = Ha$ because $aH = \{ah : h \in H\} = \{ha : h \in H\} = Ha$.

But there are non-Abelian G & $H \leq G$ such that $aH = Ha \ \forall a \in G$.

Example 1. Let $H = G$. Then there is only one coset.

Example 2. Let $G = S_n$, $H = A_n$. Then $aH = Ha \ \forall a \in S_n$.

Example 3. If $|G| = 2k$, $H \leq G$, $|H| = k$.
then $aH = Ha$ $\forall a \in G$. (e.g. D_n: dihedral group.)

Theorem 7.2 Let H, K be finite subgroups of a group. If $HK = \{hk : h \in H, k \in K\}$, then

$$|HK| = |H|\,|K|/|H \cap K|.$$

may not be a subgroup

Theorem 7.3 If G is a group with $|G| = 2p$ for a prime number $p > 2$, then G is isomorphic to the cyclic group $\mathbb{Z}_{2p}$ or the dihedral group D_p.

Another criterion for $Ha = aH \ \forall a \in G$

Fact: Theorem $H \leq G$ is normal, i.e., $Ha = aH \ \forall a \in G$

$\Leftrightarrow$ $aHa^{-1} = H$ for all $a \in G$.

Proof: ($\Rightarrow$) Assume $Ha = aH \ \forall a \in G$.

$Ha = \{ha : h \in H\}$
$= \{ah : h \in H\}$
$= aH$

for any $x = aha^{-1} \in aHa^{-1} = \{aha^{-1} : h \in H\}$.

$= (\hat{h}a)a^{-1}$ for some $\hat{h} \in H$

$= \hat{h} \in H$ $\therefore aHa^{-1} \subseteq H$.

Now To prove $H \subseteq aHa^{-1}$. $\forall a \in G$

Because $aHa^{-1} \subseteq H$

$\therefore a^{-1}(aHa^{-1})a \subseteq a^{-1}Ha$

H

So $H \subseteq a^{-1}Ha$ for any $a \in G$.

Hence $H \subseteq aHa^{-1}$. for any $a \in G$

($\Leftarrow$) Assume $aHa^{-1} = H$ for all $a \in G$

Then $(aHa^{-1})a = Ha$

aH

$\forall a \in G$