Group Theory
8th Class

I Cosets

Let G be a group, and H a subgroup. We defined an equiv. rel. on G by setting

$$a \sim b \iff ab^{-1} \in H \qquad (a, b \in G)$$

Def The equivalence classes for $\sim$ are called the right cosets of H and are denoted by Ha:

$$\begin{aligned} Ha &= \{ x \in G : x \sim a \} \\ &= \{ x \in G : xa^{-1} \in H \} \qquad xa^{-1} = h, \text{ for some } h \in H \\ &= \{ x \in G : x = ha, \text{ for some } h \in H \} \end{aligned}$$

Prop The following are equivalent (for $a, b \in G$):

(1) $Ha = Hb$
(2) $Ha \subseteq Hb$
(3) $a \in Hb$
(4) $ab^{-1} \in H$
(5) $ba^{-1} \in H$
(6) $b \in Ha$
(7) $Hb \subseteq Ha$

From discussion last time, we have

$$(*) \quad G = \coprod_{[a] \in G/\sim} Ha$$

G = disjoint union of distinct equiv. classes $\quad \coprod = \cup$

Remarks.
- When G is written additively, we write cosets as $H + a$.
- We will define similarly left cosets, aH (or $a + H$)
- When G is commutative (or abelian), $Ha = aH$ (or $a + H = H + a$)
- In general though, the left & right cosets are different

Examples

(1) $G = \mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$ (finite, abelian group)

(a) $H = \{[0], [3]\} = \langle [3] \rangle \leq G$

cosets: $[1] + H = \{[1], [4]\} = H + [1]$

$[2] + H = \{[2], [5]\} = H + [2]$

	G
H	$[0]$, $[3]$
$[1]+H$	$[1]$, $[4]$
$[2]+H$	$[2]$, $[5]$

(b) $K = \{[0], [2], [4]\} = \langle [2] \rangle \leq G$

	G
K	$[0]$, $[2]$, $[4]$
$[1]+K$	$[1]$, $[3]$, $[5]$

Remark The cosets of H are not subgroups of G (except for H itself, which is the coset of the identity)

---

(2) $G = \mathbb{Z}$, $H = 3\mathbb{Z}$ cosets: $\begin{cases} 0+3\mathbb{Z} = 3\mathbb{Z} = \{3n : n \in \mathbb{Z}\} \\ 1+3\mathbb{Z} = \{3n+1 : n \in \mathbb{Z}\} \\ 2+3\mathbb{Z} = \{3n+2 : n \in \mathbb{Z}\} \end{cases}$

---

(3) $G = \mathbb{Z}_8^\times = \{[1], [3], [5], [7]\}$

$H = \langle [3] \rangle = [3] \cdot \mathbb{Z}_8^\times = \{[3], [1]\} = \{[1], [3]\}$

$[5] \cdot H = \{[5], [7]\}$

---

(4) $G = Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ — the quaternion group of order 8

(G is a subset of $\mathbb{H}^\times$, the unit quaternions)

multiplication rules: $\begin{cases} i^2 = j^2 = k^2 = -1 \\ ij = k, \; jk = i, \; ki = j \end{cases}$

Gives mult. table

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j

$-1 \quad 1 \quad -1 \quad -k \quad k \quad j \quad -j$

$-k \quad -j, \; j$

Subgroups: $H = \{\pm 1\}$

$K = \{\pm 1, \pm i\}$

Q_8		
H	1	-1
$Hi = iH$	i	$-i$
$Hj = jH$	j	$-j$
$Hk = kH$	k	$-k$

Q_8	
K	$1 \; -1 \; i \; -i$
$Kj = jK$	$j \; -j \; k \; -k$

Left cosets

Given a subgroup $H \leq G$

Define another equiv rel on G by setting

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

[If you need to distinguish the two equiv. rels, you may write $\sim_\ell$ vs $\sim_r$]

Equiv. classes are the left cosets,

$$aH := \{x \in G : x \sim a\} = \{x \in G : x = ah \text{ for some } h \in H\}$$

As before: $bH = aH \iff bH \subseteq aH \iff b \in aH \iff a^{-1}b \in H$ etc

---

Def The number of left cosets of H equals the number of right cosets of H, and is denoted by

$$[G : H] = \#\{\text{distinct left/right cosets of } H\} \quad (**)$$

and is called the **index** of H in G.

(it is either finite or infinite)

Examples (1) $G = \mathbb{Z}_8$; $H = \{[0], [4]\}$ $\Rightarrow [G : H] = 4$

cosets are $H, [1]+H, [2]+H, [3]+H$

(2) $G = \mathbb{Z}$ $H = \{0\}$

cosets: $n + H = \{n\}$ for all $n \in \mathbb{Z}$ $\Rightarrow [G, H] = \infty$

II Lagrange's Theorem

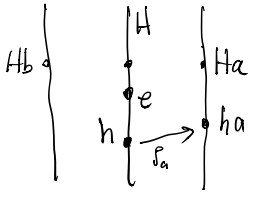
Brief history:
- First stated in a roundabout way, in a particular case, with no proof, by Lagrange in 1771
- Proved in particular cases by Gauss ($G = \mathbb{Z}_n^\times$) and Cauchy ($G = S_n$)
- Proved in general by Jordan in 1861.

Lemma All cosets of a group are in bijection to each other, or, equivalently,
Given $H \leq G$ and $a \in G$, there is a bijection

$$H \xrightarrow{f_a} Ha$$
$$h \longmapsto ha$$

and similarly, a bijection $\lambda_a : H \to aH$, $h \to ah$.

Proof



f_a injective (1-to-1): $f_a(h) = f_a(k) \Leftrightarrow ha = ka \Leftrightarrow h = k$

f_a surjective (onto): Let $ha \in Ha$. Then $ha = f_a(h)$

$\therefore f_a$ is a bijection

Alternatively, $f_a : H \to Ha$ has inverse $f_a^{-1} : Ha \to H$, $f_a^{-1}(ha) = h$ ▨

Theorem (Lagrange) Let G be a finite group, and H a subgroup. Then the order of H divides the order of G:

$$|H| \;|\; |G|$$

order of H — divides — order of G

Proof We know:

(1) $G = \bigsqcup_{[a] \in G/\sim} Ha$ (by (*))

(2) $H \longleftrightarrow Ha$ (bijection), for all a (by Lemma)

So now count:

$$|G| \overset{(1)}{=} \sum_{\text{distinct cosets of } H} |Ha| \overset{(2)}{=} \sum_{\text{distinct cosets of } H} |H| \overset{(*)}{=} |H| \cdot [G:H]$$

(*) ↑ definition of index

QED

Remarks

(1) In the proof we used right cosets. (Ha). Same proof works with left cosets (aH)

(2) The proof also shows

$$\boxed{[G:H] = \frac{|G|}{|H|}}$$

(for either the "left index" or the "right index")

(3) The converse to Lagrange's theorem is false:

[If $n \mid |G|$, there need not be a subgroup $H \leq G$ such that $|H| = n$]

Smallest such example is $G = A_4$ (the alternating group of order 12)

$\nexists\, H \leq G$ s.t. $|H| = 6$

Nevertheless, the converse is true for cyclic groups.

"Example" If $|G| = 30$, what are the possible orders of subgroups of G?

Answer: 1, 2, 3, 5, 6, 10, 15, 30

Corollary The order of any group element in a finite group G divides the order of the group.

$o(a) \mid |G|$, $\forall a \in G$

Proof Recall: $o(a) = |\langle a \rangle|$

By Lagrange: $|\langle a \rangle| \mid |G|$. So done. □

Question What are the possible orders of elements in $\mathbb{Z}_9^\times$?

Answer: $\mathbb{Z}_9^\times = \{[1], [2], [4], [5], [7], [8]\} \Rightarrow |\mathbb{Z}_9^\times| = 6$ ($= \varphi(9)$)

By Lagrange, $o(a) \in \{1, 2, 3, 6\}$, $\forall a \in \mathbb{Z}_9^\times$

$[1]$ $[8]$ $[4], [7]$ $[2], [5]$

check: $[5] \cdot [5] = [25] = [7]$ since $25 = 9 \cdot 2 + 7$

$[5] \cdot [5] \cdot [5] = [7 \cdot 5] = [35] = [8] = [-1]$

$[5]^6 = [1]$

$[7]^2 = [49] = [4]$ since $49 = 9 \cdot 5 + 4$

$[7]^3 = [28] = [1]$ since $28 = 9 \cdot 3 + 1$