§5 – Cosets & Lagrange's Theorem

In this section we prove Lagrange's theorem, an extremely important result in finite group theory, and far and away the most important result of this course. First we will need to discuss cosets.

§5.1 – Cosets

Let H be a subgroup of a group G. A left coset of H is a set obtained by "sliding" H around G. We "slide" H by multiplying it by some $a \in G$ on the left.

Ex: $3\mathbb{Z} \leq \mathbb{Z}$. The left cosets are

$$0+3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6, \ldots\} = 3\mathbb{Z}$$

$$1+3\mathbb{Z} = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$$

$$2+3\mathbb{Z} = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$$

$$3+3\mathbb{Z} = \{\ldots, -3, 0, 3, 6, 9, \ldots\} = 3\mathbb{Z}$$

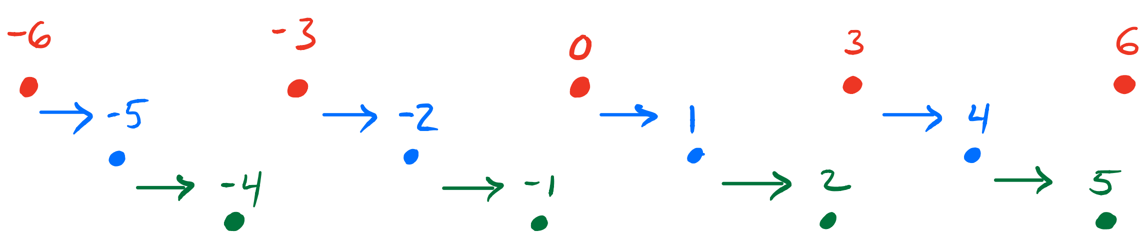
$$-1+3\mathbb{Z} = \{\ldots, -7, -4, -1, 2, 5, \ldots\} = 2+3\mathbb{Z}$$

etc...

Really, there are only 3:

$$0+3\mathbb{Z} = 3\mathbb{Z}, \quad 1+3\mathbb{Z}, \quad 2+3\mathbb{Z}.$$

They are disjoint and cover all of $\mathbb{Z}$



Ex: Consider $\langle 3 \rangle = \{0, 3\}$ in $\mathbb{Z}_6$.

Its left cosets are

$$0 + \langle 3 \rangle = \{0, 3\} = 3 + \langle 3 \rangle$$

$$1 + \langle 3 \rangle = \{1, 4\} = 4 + \langle 3 \rangle$$

$$2 + \langle 3 \rangle = \{2, 5\} = 5 + \langle 3 \rangle.$$

Remarks:

- The left cosets are either identical or disjoint
- They cover the group $\mathbb{Z}_6$
- All are the same size
- If $a \in b + \langle 3 \rangle$, then $a + \langle 3 \rangle = b + \langle 3 \rangle$.

Ex: Consider $H = \langle (1\,2\,3) \rangle$

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

as a subgroup of S_3. Its left cosets are

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

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

Exercise: Verify that in the previous example,

$$eH = (1\,2\,3)H = (1\,3\,2)H$$

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

Again, the cosets are either identical or disjoint, cover S_3, and all have the same size.

Let's formalize what we have discussed above:

Definition: Let H be a subgroup of a group G. For any $a \in G$, the set

$$\boxed{aH = \{ah : h \in H\}}$$

is a left coset of H containing a.

Similarly, we say that

$$\boxed{Ha = \{ha : h \in H\}}$$

is a right coset of H containing a.

The index of H in G, denoted by $|G:H|$ is the number of left (equivalently, right) cosets of H in G.

Proposition 5.1: Let $a, b \in G$, $H \leq G$.

(1) $a \in aH$

(2) $aH = bH \iff a \in bH$

[In particular, $aH = H \iff a \in H$]

(3) $aH = bH$ <u>or</u> $aH \cap bH = \emptyset$.

(4) $aH = bH \iff a^{-1}b \in H$

(5) $|aH| = |H|$

Analogous statements hold for right cosets.

(6) $aH = Ha \iff aHa^{-1} = H$

Proof: (1) $a = ae \in H$

(2) If $aH = bH$ then $a \in aH = bH$

Now suppose that $a \in bH$, so $a = bh$ for some $h \in H$. We have that

$$aH = (bh)H = b(hH) = bH.$$

(3). Suppose $aH \cap bH \neq \emptyset$, so $\exists c \in aH \cap bH$.

Then $c \in aH \Rightarrow aH = cH$ (by (2))

and $c \in bH \Rightarrow bH = cH$ (by (2)).

Thus, $aH = bH$.

(4) $aH = bH \Leftrightarrow b \in aH$ (by (2))

$\Leftrightarrow b = ah$ for some $h \in H$

$\Leftrightarrow a^{-1}b \in H$.

(5) Note that $aH = \varphi_a(H)$, where $\varphi_a : G \to G$ maps g to $a \cdot g$. On A1 you proved that φ_a is bijective. Hence $|aH| = |H|$.

(6) Exercise. $\blacksquare$

Remarks:

- (1) says that every element of G is in some coset.
- (3) says that cosets are identical or disjoint.
- (5) says that all cosets are the same size.

These statements will be the key to proving Lagrange's Theorem.

§ 5.2 - Lagrange's Theorem & its Consequences

In § 5.1 we proved that if $H \leq G$, then

(i) Every element of G is in some coset;

(ii) Cosets are identical or disjoint

(iii) All cosets have size $|H|$.

Suppose now that G is a finite group with $H \leq G$. Let $a_1 H, a_2 H, \ldots, a_k H$ be the distinct left cosets of H in G (here,

$$\boxed{K = \# \text{ of left cosets } = |G : H|}$$

By (i), $G = a_1 H \cup a_2 H \cup \cdots \cup a_k H$

By (ii), $a_i H \cap a_j H = \emptyset \quad \forall i \neq j$

$$\begin{aligned} \text{Thus, } |G| &= |a_1H| + |a_2H| + \cdots + |a_kH| \\ &= |H| + |H| + \cdots + |H| \quad \text{(by (iii))} \\ &= k|H| \end{aligned}$$

We have just proved the most important theorem of the course:

Lagrange's Theorem If G is a finite group and $H \leq G$, then $|H|$ divides $|G|$

Although easy to state and prove, this theorem leads to several amazing corollaries.

Corollary 1: If G is a finite group and $H \leq G$, then $|G:H| = |G|/|H|$

Proof: In the proof of Lagrange's theorem, we saw $|G| = k|H|$ where $k = |G:H|$. Thus, $|G:H| = |G|/|H|$. ■

Corollary 2: If G is a finite group and $a \in G$, then $|a|$ divides $|G|$.

Proof: $|a| = |\langle a \rangle|$, and this divides $|G|$ by Lagrange's theorem. ■

Corollary 3: If G is a finite group and $a \in G$, then $a^{|G|} = e$.

Proof: Immediate from Corollary 2. ■

Corollary 4: If p is a prime and G is a group of order p, then G is cyclic.

Proof: Let $a \in G \setminus \{e\}$. Since $|a|$ divides $|G| = p$ (prime), $|a| = 1$ or p. Since $a \neq e$, $|a| \neq 1$. Thus, $|a| = p$ so $\langle a \rangle = G$. ■

Corollary 5 [Fermat's Little Theorem] If p is a prime and a is an integer with $p \nmid a$, then $a^{p-1} \equiv 1 \mod p$.

Proof: Since $p \nmid a$, $\gcd(a, p) = 1$, and hence $a \in \mathbb{Z}_p^* = \{1, 2, \dots, p-1\}$. Thus, by Corollary 3, $a^{p-1} = 1 \mod p$. $\blacksquare$

Remark: Lagrange's theorem states that the order of a subgroup of a finite group G divides $|G|$, but it does NOT guarantee that there is a subgroup of order d for every positive divisor d of $|G|$ (though this is true when G is cyclic)

Ex: $|A_4| = 12$, but A_4 has no subgroup of order 6.

Why? Suppose H were such a subgroup. Since A_4 contains 8 elements of order 3, at least one $a \in A_4$ of order 3 is not in H. Thus,

$A_4 = H \cup aH$.

Which coset contains a^2? If $a^2 \in H$, then so is $(a^2)^2 = a^4 = a$ $\#$. Thus, $a^2 \in aH$. This then means that $a^2 = ah$ for some $h \in H$, and hence $a = h \in H$ $\#$.

Thus, there is no subgroup of order 6.

Theorem 5.2: Let H and K be finite subgroups of a group G, and define the set $HK = \{hk : h \in H, k \in K\}$. Then

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

Proof: There are $|H||K|$ products in HK, but some of these products may represent the same element.

Note that if $b \in H \cap K$, then for $h \in H$, $k \in K$, we have $hk = \underbrace{(hb)}_{\in H}\underbrace{(b^{-1}k)}_{\in K}$, so every product has been counted at least $|H \cap K|$ times.

But if $hk = h'k'$, then $b = h^{-1}h' = kk'^{-1}$ belongs to $H \cap K$. We then have that $h' = hb$ and $k' = b^{-1}k$ (i.e., the only other way to write hk is $h'k' = (hb)(b^{-1}k)$ for some $b \in H \cap K$.

Thus, every element of HK is counted $|H \cap K|$ times, so $|HK| = \dfrac{|H||K|}{|H \cap K|}$ $\blacksquare$

Remark: In general, HK is just a set!

It is not necessarily a subgroup.

e.g. $H = \langle (12) \rangle = \{e, (12)\} \leq S_3$

$K = \langle (13) \rangle = \{e, (13)\} \leq S_3$

Then $|HK| = \dfrac{|H||K|}{|H \cap K|} = \dfrac{2 \cdot 2}{1} = 4.$

Since $4 \nmid 6$, HK is NOT a subgroup of S_3.

Ex: If G is a group of order 100, then G has exactly one subgroup of order 25.

Indeed, suppose H & K are distinct subgroups of G with $|H| = |K| = 25$.

Since $H \neq K$, we have $H \neq H \cap K \neq K$.

Thus, since $H \cap K$ is a subgroup of H and K, $|H \cap K| = 1$ or 5 (Lagrange).

Hence $|HK| = \dfrac{|H||K|}{|H \cap K|} = \dfrac{625}{1}$ or $\dfrac{625}{5} = 125$.

This is a contradiction, as $HK \subseteq G$ and $|G| = 100$.

Application to Rubik's Cubes

How big is the group of symmetries of the Rubik's cube? Call this group R. Note that R is a subgroup of R', the group of symmetries of the Rubik's cube where disassembling the cube is allowed.

Note that the Rubik's cube has 8 corner pieces and 12 edge pieces (the 6 middle pieces are fixed and cannot be removed). The

8 corner pieces can be permuted in $8!$ ways and each rotated in 3 ways, while the 12 edge pieces can be permuted in $12!$ ways and each flipped in 2 ways. Thus,

$$|R'| = 8! \cdot 3^8 \cdot 12! \cdot 2^{12}.$$

By Lagranges theorem, $|R|$ divides $8! \cdot 3^8 \cdot 12! \cdot 2^{12}$.

It can be shown using some Rubik's cube knowledge that $|R' : R| = 12$, so $\frac{|R'|}{|R|} = 12$.

So $|R| = \frac{|R'|}{12} = \boxed{\begin{aligned} &8! \cdot 3^8 \cdot 11! \cdot 2^{12} \\ &= 43{,}252{,}003{,}274{,}489{,}856{,}000. \end{aligned}}$

($\approx$ 43 quintillion elements)