Lecture 18: Cosets & Lagrange's Theorem

Contents

In this lecture we introduce a powerful tool for analyzing a group - a *coset*. We'll then use cosets to prove Lagrange's Theorem (discussed in Lecture 11) which states the size of a subgroup divides the size of the group.

18.1 Cosets

Let H be a subgroup of a group G. Define a relation $\sim_H$ on G as follows:

$$a \sim_H b \iff a^{-1}b \in H. \tag{1}$$

Equivalently, $a \sim_H b$ if and only if $a^{-1}b = h$ for some $h \in H$. Or another way to say this is $a \sim_H b$ if and only if $b = ah$ for some $h \in H$.

Lemma 18.1 *If $H < G$, then $\sim_H$ is an equivalence relation on G. Moreover, if $[a]$ denotes the equivalence class of $a \in G$, then*

$$[a] = \{ah \mid h \in H\}.$$

Proof: We need to show $\sim_H$ is reflexive, symmetric and transitive. For all $a, b, c \in G$:

Reflexive: Since H is a subgroup it contains the identity, so $a^{-1}a = e \in H$, Therefore, $a \sim_H a$.

Symmetric: If $a \sim_H b$ then $a^{-1}b \in H$. Since H is a subgroup it is closed under taking inverses, so $(a^{-1}b)^{-1} = b^{-1}a \in H$. Therefore $b \sim_H a$.

Transitive: If $a \sim_H b$ and $b \sim_H c$ then $a^{-1}b, b^{-1}c \in H$. Since H is a subgroup it is closed under products, so $(a^{-1}b)(b^{-1}c) = a^{-1}c \in H$. Therefore $a \sim_H c$.

It follows that $\sim_H$ is an equivalence relation on G.

Since $a \sim_H b$ if and only if $b = ah$ for some $h \in H$, then

$$\begin{aligned}[a] &= \{b \mid a \sim_H b\} \\ &= \{ah \mid h \in H\}\end{aligned}$$

□

The following definition gives a name to the particular type of equivalence class that appeared in the lemma.

Definition 18.1 (Coset of H in G) *Let G be a group and H a subgroup 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. Analogously,*

$$Ha = \{ha \mid h \in H\}$$

*is called the **right coset of** H in G containing a. The element a is called the **coset representative of** aH or Ha.*

The *right coset* is the equivalence class that comes from the equivalence relation $a \sim b$ if and only if $ab^{-1} \in H$.

Since left cosets of H are the equivalence classes under the relation $\sim_H$ they form a partition of the group G. In particular, for any two left cosets aH and bH we either have

$$aH = bH \quad \text{or} \quad aH \cap bH = \emptyset.$$

Let's see what these cosets look like in a few specific examples.

Example 18.1 *Let $S_3 = \{\varepsilon, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$, and consider the subgroup $H = \langle (1,2) \rangle = \{\varepsilon, (1,2)\}$. The left cosets of H are:*

$$\begin{aligned} \varepsilon H = H &= \{\varepsilon, (1,2)\} \\ (1,3)H &= \{(1,3), (1,3)(1,2)\} = \{(1,3), (1,3,2)\} \\ (2,3)H &= \{(2,3), (2,3)(1,2)\} = \{(2,3), (1,2,3)\} \end{aligned}$$

The left coset representatives of H in G are therefore $\varepsilon, (1,3)$, and $(2,3)$.

Notice that

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

In other words, it doesn't matter which element of the coset you use to describe it. For instance, $(1,2), (1,3,2), (1,2,3)$ is another set of left coset representatives of H in G.

The right cosets of H are:

$$\begin{aligned} H\varepsilon = H &= \{\varepsilon, (1,2)\} \\ H(1,3) &= \{(1,3), (1,2)(1,3)\} = \{(1,3), (1,2,3)\} \\ H(2,3) &= \{(2,3), (1,2)(2,3)\} = \{(2,3), (1,3,2)\} \end{aligned}$$

Notice that the left and right cosets are not necessarily the same. For example $(1,3)H \neq H(1,3)$.

For the subgroup $K = \langle (1,2,3) \rangle = \{\varepsilon, (1,2,3), (1,3,2)\}$ there are only two distinct left cosets:

$$\begin{aligned} K &= \{\varepsilon, (1,2,3), (1,3,2)\} \\ (1,2)K &= \{(1,2), (1,2)(1,2,3), (1,2)(1,3,2)\} = \{(1,2), (1,3), (2,3)\}. \end{aligned}$$

Notice that $K = (1,2,3)K = (1,3,2)K$ and $(1,2)K = (1,3)K = (2,3)K$.

Example 18.2 *Consider C_{12}, the group of integers modulo 12, and the subgroup $H = \langle 3 \rangle = \{0,3,6,9\}$. The cosets of H are:*

$$\begin{aligned} 0 +_{12} H &= H = \{0,3,6,9\} \\ 1 +_{12} H &= \{1,4,7,10\} \\ 2 +_{12} H &= \{2,5,8,11\} \end{aligned}$$

Note that the left and right cosets are the same in this case since C_{12} is abelian. Also,

$$1 +_{12} H = 4 +_{12} H = 7 +_{12} H = 10 +_{12} H.$$

In each of the examples above notice that the only coset of H which is a subgroup of G is H itself. Here are some basic properties of cosets.

Lemma 18.2 (Properties of Cosets) *Let H be a subgroup of G and $a \in G$.*

(a) $a \in aH$

(b) $aH = H \iff a \in H$

(c) For $a, b \in G$, either $aH = bH$ or $aH \cap bH = \emptyset$.

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

(e) If G is finite then $|H| = |aH|$

(f) $aH = Ha \iff a^{-1}Ha = H.$

(Note that by $a^{-1}Ha$ we mean the set $\{a^{-1}ha \mid h \in H\}$.)

Proof: First observe that since aH is the equivalence class $[a]$ then (a), (c), and (d) are just the results of Lemma 17.1 which we have already proven.

(b) If $aH = H$ then $a \in aH = H$. Conversely, suppose $a \in H$. Then $aH \subset H$, while on the other hand, if $b \in H$ then $a^{-1}b \in H$ so $b \in aH$. Therefore $aH = H$.

Another way to prove this is to just observe that it is a special case of (d) where $b = e$. Therefore it follows as a direct consequence of Lemma 17.1.

(e) The map $\psi : H \to aH$ defined by

$$\psi(h) = ah,$$

is a bijection.
Injective: $\psi(h_1) = \psi(h_2)$ implies $ah_1 = ah_2$, and by cancellation, $h_1 = h_2$.
Surjective: For $b \in aH$, there is an $h \in H$ such that $b = ah$. Therefore, $a^{-1}b \in H$ and $\psi(a^{-1}b) = b$.

Since ψ is a bijection then H and aH must have the same size: $|H| = |aH|$.

(f) ($\Longrightarrow$) If $aH = Ha$ then for any $h \in H$ there is an $x \in H$ such that $ax = ha$, so $a^{-1}ha \in H$. Therefore $a^{-1}Ha \subset H$. On the other hand, for any $h \in H$ there is a $y \in H$ such that $ah = ya$, so $h = a^{-1}ya \in a^{-1}Ha$. Therefore $H \subset a^{-1}Ha$. It follows that $H = a^{-1}Ha$.

($\Longleftarrow$) If $a^{-1}Ha = H$ then for any $h \in H$ there is an $x \in H$ such that $a^{-1}xa = h$, so $ah = xa \in Ha$. Therefore $aH \subset Ha$. A similar argument shows $Ha \subset Ha$. Therefore $aH = Ha$. □

18.2 Lagrange's Theorem

We stated Lagrange's Theorem back in Lecture 11. Now we have the tools to prove it.

Theorem 18.1 (Lagrange's Theorem) *If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$.*

Proof: Let $\sim_H$ be the equivalence relation on G defined in (1). Then the equivalence classes are the left cosets $[a] = aH$. Let

$$a_1H, a_2H, \ldots, a_kH$$

denote the distinct left cosets of H in G. By Lemma 18.2(e) all equivalence classes have the same size: $|[a_i]| = |a_iH| = |H|$. Since these classes partition G then

$$G = a_1H \cup a_2H \cup \cdots \cup a_kH, \quad \text{(disjoint union)}$$

and so

$$|G| = |a_1H| + |a_2H| + \cdots + |a_kH| = k|H| \tag{2}$$

Therefore $|H|$ divides $|G|$. □

From Equation (2) we have a formula for the number of left cosets of H in G:

$$\text{number of left cosets} \quad = \quad \text{number of } \sim_H \text{ equivalence classes} \quad = \quad \frac{|G|}{|H|}.$$

Similarly, working with right cosets rather than left cosets in our previous arguments, we have that the number of right cosets is also $|G|/|H|$.

In particular, the *number* of left and right cosets of a given subgroup are the same. This is an important number in calculations involving groups and is called the **index of H in G**, which is denoted by $[G/H]$:

$$[G/H] := \text{ the index of } H \text{ in } G \ = \frac{|G|}{|H|}. \tag{3}$$

However, even though the *number* of left and right cosets of a subgroup H in G is the same, the actual left and right cosets themselves can be different. See Example 18.1.

In Lecture 11 we noted a few consequences of Lagrange's Theorem. We'll list them here again for convenience.

Corollary 18.1 ($ord(a)$ divides $|G|$) *Let G be a finite group and $a \in G$. Then*

(a) *$ord(a)$ divides $|G|$.*

(b) *$a^{|G|} = e$.*

Example 18.3 (Number of different cubes up to U, R moves) *In Example 17.1 we considered the set $\mathcal{C}$ of all the different configurations of Rubik's cube and the equivalence relation $\equiv$ on $\mathcal{C}$ defined by*

$$X \equiv Y \iff \begin{array}{l}\textit{if there is a sequence of moves involving only } U \textit{ and } R \\ \textit{that takes configuration } X \textit{ to configuration } Y.\end{array}$$

If we identify each configuration in $\mathcal{C}$ with its corresponding permutation in RC_3, the the equivalence relation $\equiv$ can be described as

$$X \equiv Y \iff X^{-1}Y \in H = \langle U, R \rangle$$

In other words, it is just the relation $\sim_H$, and so the equivalence classes are the cosets of $H = \langle U, R \rangle$.

If X_0 denotes the cube in the solved state, then $[X_0] = H$, and as we found in Example 17.1, has size $73,483,200$. The number of distinct equivalence classes is given by (3), and we can use SAGE to compute it.

SAGE

```
sage: S48=SymmetricGroup(48)
sage: R=S48("(25,27,32,30)(26,29,31,28)(3,38,43,19)(5,36,45,21)(8,33,48,24)")
sage: L=S48("(9,11,16,14)(10,13,15,12)(1,17,41,40)(4,20,44,37)(6,22,46,35)")
sage: U=S48("(1,3,8,6)(2,5,7,4)(9,33,25,17)(10,34,26,18)(11,35,27,19)")
```

```
sage: D=S48("(41,43,48,46)(42,45,47,44)(14,22,30,38)(15,23,31,39)(16,24,32,40)")
sage: F=S48("(17,19,24,22)(18,21,23,20)(6,25,43,16)(7,28,42,13)(8,30,41,11)")
sage: B=S48("(33,35,40,38)(34,37,39,36)(3,9,46,32)(2,12,47,29)(1,14,48,27)")
sage: RC3=S48.subgroup([R,L,U,D,F,B])
sage: H=S48.subgroup([R,U])
sage: RC3.order()/H.order()
588597166080
```

What does this mean? It means that if we think of any two configurations, in which one can be obtained from the other by only twisting the R and U faces, as equivalent, then we've partitioned $\mathcal{C}$ into $588,597,166,080$ sets, each of size $73,483,200$, where within each set of the partition any two configurations are equivalent under U, R moves. But for any two configurations coming from different sets in the partition, there is now way to obtain one from the other using U, R moves. In this sense there are $588,597,166,080$ different *cubes up to R, U moves.*

An Application to Number Theory:

We briefly look at how our previous results can be used to establish two very famous theorems of number theory.

Corollary 18.2 (Fermat's Little Theorem) *For every integer a and every prime p,*

$$a^p \equiv a \pmod{p}.$$

That is, p divides $a^p - a$.

Proof: Let r be the remainder of a upon division by p. Since $a \equiv r \pmod{p}$ and $a^p \equiv r^p \pmod{p}$ then it suffices to prove the corollary for $0 \leq a \leq p-1$. The result for $a = 0$ is trivial. So assume $1 \leq a \leq p-1$. Then we can assume $a \in U(p)$, the groups of integers $\{1, 2, \ldots, p-1\}$ under multiplication modulo p. (See Lecture 10 for further discussion of $U(n)$.) Since $|U(p)| = p-1$ then by Corollary 18.1 $a^{p-1} \equiv 1 \pmod{p}$, therefore $a^p \equiv a \pmod{p}$. □

For example, without doing any calculation we know that $2011^{13} - 2011$ is divisible by 13.

Corollary 18.3 (Euler's Theorem) *Let $a \in \mathbb{Z}$, $n \in \mathbb{Z}_+$ and $\gcd(a, n) = 1$. Then*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Proof: It suffices to prove the result for $0 < a < n$, since $a^k \equiv r^k \pmod{n}$ for any $k \in \mathbb{N}$, where r is the remainder of a when divided by r. Since $\gcd(a, n) = 1$ then $a \in U(n)$, the multiplicative group of units modulo n. Since $|U(n)| = \phi(n)$ (Euler's phi-function) then by Corollary 18.1(b) it follows that

$$a^{\phi(n)} = a^{|U(n)|} \equiv 1 \pmod{n}.$$

□

18.3 Exercises

1. Consider the group C_{12} and the subgroup $H = \langle 4 \rangle = \{1, 4, 8\}$.

   (a) Are the following pairs of elements related under $\sim_H$?

(i) $3, 7$ (ii) $5, 11$ (iii) $6, 9$

(b) Find all (left) cosets of H in G.

2. In S_7, are the following pairs of elements related under $\sim_H$ where $H = A_7$?

(a) $(1,2)(3,4)(5,6)$, $(1,7)(2,6)(3,5)(4,7)$.
(b) $(2,3)(4,6)$, $(1,3,5,7,4)$.
(c) $(1,3,7,2)$, $(2,4,3,6,5)$.

3. Let $H = \{\varepsilon, (1,3)\}$ in S_3.

(a) Find all the left cosets of H.
(b) Find all the right cosets of H.

4. Let H and K be subgroups of a group G such that $\gcd(|H|, |K|) = 1$. Show that $|H \cap K| = 1$.

5. Let G be a group such that $|G| = 35$.

(a) Show that G has at most 8 subgroups of order 5.
(b) Show that G has at most 5 subgroups of order 7.
(c) Deduce that G has at least one element of order 5 and at least one element of order 7.

6. Let H be a subgroup of a group G with $|H| = \frac{1}{2}|G|$.

(a) Show that $a \notin H$ implies $G = H \cup aH$.
(b) Show that $a \notin H$ implies $a^n H \neq a^{n+1} H$.
(c) Deduce that H contains every element in G of odd order.

7. (a) How many 3-cycles are there in A_5?
(b) How many 5-cycles are there in A_5?
(c) Use Exercise 6 to show that A_5 has no subgroup of order 30.

8. Repeat the argument of Exercise7 (modifying it where appropriate) to show that A_4 has no subgroup of order 6.