Lecture 7: Lagrange's Theorem

Theorem

(Lagrange's Theorem) Let G be a finite group with a subgroup H. Then the order of H divides the order of G.

Notes

1. Recall that "divides" means "is a factor of". The symbol for "divides" is a vertical bar. For example "$3|21$" is the statement that 3 is a divisor of 21.
2. Lagrange's Theorem says that a subgroup of S_4, which has $4! = 24$ elements, could possibly have $1, 2, 3, 4, 6, 8, 12$ or 24 elements, but couldn't have (for example) 7 or 16 elements.
3. The converse of Lagrange's Theorem is not true; if n and k are integers and $k|n$, it is not true that every group of order n has a subgroup of order k.

Left cosets

Definition Let H be a subgroup of a group G (with binary operation $\star$). Then the left coset of H in G determined by x, which is denoted xH or $x \star H$, is the set $xH = \{x \star h : h \in H\}$.

Notes

1. xH consists of the elements of H, all "translated" by being composed on the left with the element x. We can think of it as a "shifted copy" of H inside G.
2. xH is a subset of G, generally not a subgroup.
3. It is possible for two different elements x and y of G to determine the same left coset of H. For example if x is any element of the subgroup H, then xH is just H itself.
4. There is a corresponding concept of right coset, which we will care about later but not now. The right coset of H determined by x would be $Hx = \{hx : h \in H\}$.

Examples of Left Cosets

If G is the group of integers under addition, and H is a subgroup $5\mathbb{Z}$ consisting of all multiples of 5, then the left coset of H in G determined by 3 is

$$\begin{aligned} 3+H &= \{\ldots, 3+(-5), 3+0, 3+5, 3+10, \ldots\} \\ &= \{\ldots, -2, 3, 8, 13, \ldots\} \\ &= 3+5\mathbb{Z}. \end{aligned}$$

This is the congruence class of 3 modulo 5. Note that $3, 8, -2, -7$ all determine the same coset (they are all congruent to each other modulo 5).

Examples of Left Cosets

If G is $\mathrm{GL}(2,\mathbb{Q})$, the group of all 2×2 rational matrices under matrix multiplication, and H is the subgroup $\mathrm{SL}(2,\mathbb{Q})$ consisting of all matrices of determinant 1, then the left coset of H in G determined by $\begin{pmatrix} 2 & 3 \\ 4 & 3 \end{pmatrix}$ is

$$\left\{ \begin{pmatrix} 2 & 3 \\ 4 & 3 \end{pmatrix} B : \det(B) = 1 \right\}.$$

This set consists of all matrices in $\mathrm{GL}(2,\mathbb{Q})$ whose determinant is -6.

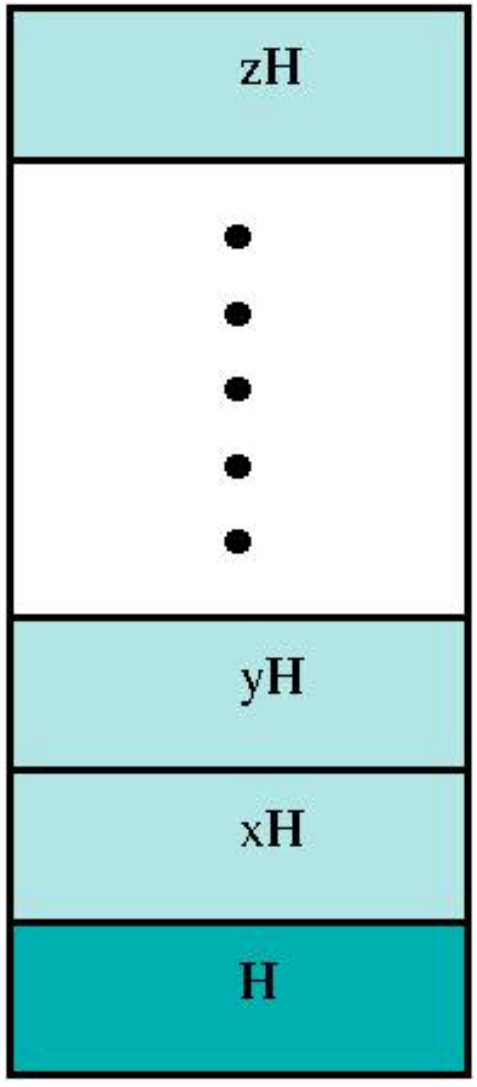
Examples of Left Cosets

If G is the dihedral group D_8 consisting of symmetries of the square, and H is the subgroup of G consisting of the four rotations, then the left coset of H in G determined by any one of the four reflections consists of the four reflections. The left coset of H in G determined by any one of the four rotations consists of the four rotations.

Note that there are only two distinct cosets, they have empty intersection and their union is the whole group G.

Proof Mechanism for Lagrange's Theorem

Start with the subgroup H of the finite group G.
If $H = G$ the theorem holds.
If not, choose an element x of G with $x \notin H$.
Then the coset xH is disjoint from H and has $|H|$ elements.
If $H \cup xH = G$ then $|G| = 2|H|$ and we are done.
If not, choose $y \notin H \cup xH$ and add the coset yH.
Eventually we find that G is the union of k disjoint left cosets of H, and $|G| = k|H|$.



Proof of Lagrange's Theorem

Recall these two items from Lecture 7:

Theorem

(Lagrange's Theorem) Let G be a finite group with a subgroup H. Then the order of H divides the order of G.

Definition Let H be a subgroup of a group G (with binary operation $\star$). Then the left coset of H in G determined by x, which is denoted xH or $x \star H$, is the set

$$xH = \{x \star h : h \in H\}.$$

Key property of left cosets

This is Lemma 2.1.5 in the lecture notes.

Lemma Suppose that g_1 and g_2 are elements of a group G and that H is a subgroup of G. Then either the cosets g_1H and g_2H are equal to each other or they are disjoint from each other, i.e. their intersection is empty, they have no element in common.

Note: Since g_1H and g_2H are *sets* (subsets of G), what it means to say that they are equal is that they have exactly the same elements. A standard way to show that two sets A and B are equal is to show that every element of A belongs to B (so $A \subseteq B$) and that every element of B belongs to A (so $B \subseteq A$).

Proof

If g_1H and g_2H have no element in common then there is nothing to do.

So suppose that these two sets *do* have at least one element in their intersection. This means that there are elements h_1 and h_2 of H for which

$$g_1h_1 = g_2h_2.$$

We must deduce that the sets g_1H and g_2H are equal.

First we show that $g_1H \subseteq g_2H$.

Choose an element of g_1H. It is g_1h for some $h \in H$.

Now

$$g_1h_1 = g_2h_2 \Longrightarrow g_1 = g_2h_2h_1^{-1},$$

so we can write $g_1h = g_2h_2h_1^{-1}h = g_2\underbrace{(h_2h_1^{-1}h)}_{\in H}$.

So $g_1h \in g_2H$ and $g_1H \subseteq g_2H$.

Proof (continued)

Starting with $g_1 h_1 = g_2 h_2$ and rewriting it as $g_2 = g_1 h_1 h_2^{-1}$, we can use the same approach to prove the oppostite inclusion $g_2 H \subseteq g_1 H$. We conclude that the left cosets of H determined by different elements of G are identical if they intersect at all. □

It is this property that allows to prove Lagrange's Theorem by establishing that G is the union of the distinct left cosets of H, each of which has the same number of elements as H. The number of these cosets is called the index of H in G, denoted by $[G : H]$. If G is finite, then

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