Section 10 – Cosets and the Theorem of Lagrange

Instructor: Yifan Yang

Fall 2006

Outline

Cosets

Theorem of Lagrange

Cosets

Theorem (10.1)

Let H be a subgroup of G. Let the relation $\sim_L$ on G be defined by

$$a \sim_L b \quad \Leftrightarrow \quad a^{-1}b \in H,$$

and the relation $\sim_R$ be defined by

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

Then $\sim_L$ and $\sim_R$ are both equivalence relations on G.

Cosets

Proof.

Here we only prove the $\sim_R$ case. We need to show

1. Reflexive: We need to show that aa^{-1} is in H. We have $aa^{-1} = e$. Since H is a subgroup, H contains $e = aa^{-1}$.
2. Summetric: We need to show that $ab^{-1} \in H$ implies $ba^{-1} \in H$. Now $ba^{-1} = (ab^{-1})^{-1}$. Because H is a subgroup, if ab^{-1} is in H, so is its inverse $(ab^{-1})^{-1} = ba^{-1}$.
3. Transitive: We need to show that if $ab^{-1}, bc^{-1} \in H$, then so is ac^{-1}. We have $ac^{-1} = (ab^{-1})(bc^{-1})$. Since H is a subgroup, if ac^{-1} and bc^{-1} are in H, so is their product $(ab^{-1})(bc^{-1}) = ac^{-1}$.

This completes the proof. $\square$

Cosets

Definition
Let H be a subgroup of a group G. The equivalence class $\{b \in G : a \sim_L b\}$ is called the left coset of H containing a. Likewise, the equivalence class $\{b \in G : a \sim_R b\}$ is called the right coset of H containing a.

Remark
It is straightforward to see that the left coset of H containing a is exactly $aH = \{ah : h \in H\}$, and the right coset of H containing a is $Ha = \{ha : h \in H\}$. This is why $\sim_L$ is *left* and $\sim_R$ is *right*.

Examples

Let $G = \mathbb{Z}$ and $H = 3\mathbb{Z}$. We have

$$m \sim_L n \;\Leftrightarrow\; (-m) + n \in H \;\Leftrightarrow\; 3|(n - m).$$

Thus, a left coset of $3\mathbb{Z}$ is just a residue class modulo 3. There are three distinct left cosets $3\mathbb{Z}$, $1 + 3\mathbb{Z}$, and $2 + 3\mathbb{Z}$. Similarly, we have

$$m \sim_R n \;\Leftrightarrow\; m + (-n) \in H \;\Leftrightarrow\; 3|(m - n).$$

Again, we find that a right coset of $3\mathbb{Z}$ is just a residue class modulo 3. In this case, we see that left cosets and right cosets are the same. Also, $m + 3\mathbb{Z} = 3\mathbb{Z} + m$ for all $m \in \mathbb{Z}$.

Examples

Let $G = \mathbb{Z}_6$ and $H = \{\bar{0}, \bar{3}\}$. The left cosets are $\bar{m} + H$ for $\bar{m} \in \mathbb{Z}_6$. We find that they are $H = \{\bar{0}, \bar{3}\}$, $\bar{1} + H = \{\bar{1}, \bar{4}\}$, and $\bar{2} + H = \{\bar{2}, \bar{5}\}$. The right cosets are $H + \bar{m}$. In this case, we find that left cosets are also right cosets, and $\bar{m} + H = H + \bar{m}$.

Examples

Let $G = S_3 = \{e, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$ and $H = \{e, (1,2)\}$. The left cosets are $H = \{e, (1,2)\}$ itself,

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

and

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

The right cosets are H itselft, $H(1,3) = \{(1,3), (1,2)(1,3)\} = \{(1,3), (1,3,2)\}$, and $H(2,3) = \{(2,3), (1,2)(2,3)\} = \{(2,3), (1,2,3)\}$. In this case, we find $(1,3)H \neq H(1,3)$ and $(2,3)H \neq H(2,3)$. In fact, the subset $(1,3)H = \{(1,3), (1,2,3)\}$ is a left coset, but not a right coset.

Examples

Let $G = S_3$ and $H = \{e, (1,2,3), (1,2,3)^2 = (1,3,2)\}$. The left cosets are H itself and

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

The right cosets are H and

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

In this case, we find that each left coset is also a right coset and $\sigma H = H\sigma$ for all $\sigma \in S_3$.

Remark

1. If a group G is abelian and H is a subgroup, then each left coset is also right coset. In fact, we have

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

   In this case, we simply call a left or right coset a coset.
2. If H is a subgroup of a non-abelian group G, then a left coset of H may or may not be a right coset of H.

In-class exercises

1. Let $G = \mathbb{Z}_{12}$ and $H = \langle \bar{3} \rangle$. Find all the cosets of H.
2. Recall that the 4-th dihedral group D_4 is given by $\{e, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$, where σ and τ satisfy $\sigma^4 = \tau^2 = e$ and $\sigma\tau = \tau\sigma^3$. Let $G = D_4$ and $H = \{e, \tau\}$. Find all the left cosets of H.
3. Let $G = D_4$ and $H = \{e, \tau\}$. Find all the right cosets of H.

Theorem of Lagrange

Lemma

Let H be a subgroup of a finite group G. Then every coset (either left or right) has the same number of elements as H

Proof.

Let $a \in G$. We will prove $|H| = |aH|$ by constructing a one-to-one and onto function from H to aH. A natural function to consider is $\phi : H \to aH$ defined by $\phi(h) = ah$ for all $h \in H$. We verify that it is

1. one-to-one: Suppose that $\phi(h_1) = \phi(h_2)$. Then $ah_1 = ah_2$. By the left cancellation law, it implies that $h_1 = h_2$. Thus ϕ is one-to-one.
2. onto: It is obvious from the definition of aH.

□

Theorem of Lagrange

Theorem (10.10, Theorem of Lagrange)

Let H be a subgroup of a finite group G. Then the order of H divides the order of G.

Proof.

Since $\sim_L$ is an equivalence relation, the left cosets of H form a partition of G (i.e., each element of G is in exactly one of the cells). By the above lemma, each left coset contains the same number of elements as H. Thus

$$|G| = |H| \times \text{(the number of left cosets)}.$$

This proves the theorem. $\square$

The Lagrange theorem

Theorem (10.12)

The order of an element of a finite group divides the order of the group.

Proof.

Let $a \in G$. Apply the Lagrange theorem to $H = \langle a \rangle$. We have $|\langle a \rangle| \Big| |G|$. □

Corollary 10.11

Every group of prime order is cyclic.

Proof.

Let $g \in G$ be an element not equal to e. Then $|\langle g \rangle|$ divides the order of G. Since $|G|$ is a prime, either $|\langle g \rangle| = 1$ or $|G|$. The former case can not occur because $g \neq e$. Then $|\langle g \rangle| = |G|$ implies $\langle g \rangle = G$, i.e., G is cyclic. $\square$

Index

Definition
Let H be a subgroup of a group G. The number of left cosets of H is the index of H in G, and is denoted by $(G : H)$.

Theorem (10.14)
Suppose that H and K are subgroups of a group G such that $K \leq H \leq G$. Suppose that $(G : H)$ and $(H : K)$ are finite. Then $(G : K)$ is also finite and $(G : K) = (G : H)(H : K)$.

Proof.
Exercise 38. □

Applications

Find all the subgroups of S_3.

Solution. Since $|S_3| = 6$, by the Lagrange theorem, the possible orders of a subgroup H are 1, 2, 3, and 6.

1. Case $|H| = 1$: $H = \{e\}$.
2. Case $|H| = 2$: Since every group of order 2 is isomorphic to the cyclic group $\mathbb{Z}_2$, $H = \langle \sigma \rangle$ for some elements σ of order 2. There are three such elements, namely, $(1, 2)$, $(1, 3)$, and $(2, 3)$. Thus, there are three subgroups of order 2. They are $\{e, (1, 2)\}$, $\{e, (1, 3)\}$, and $\{e, (2, 3)\}$.
3. Case $|H| = 3$: By the same token, every subgroup of order 3 is cyclic. There are two elements of order 3, namely, $(1, 2, 3)$ and $(1, 3, 2)$. They both generate $\{e, (1, 2, 3), (1, 3, 2)\}$.
4. Case $|H| = 6$: In this case, $H = S_3$.

Thus, we see that S_3 has 6 subgroups. $\square$

Applications

Find all the subgroups of $D_4 = \{e, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$.
Solutions. The possible orders are 1, 2, 4, and 8.

1. Case $|H| = 1$: We have $H = \{e\}$.
2. Case $|H| = 2$: Again $H = \langle g \rangle$ for some elements g of order 2. There are 5 elements of order 2. They are σ^2, τ, $\sigma\tau$, $\sigma^2\tau$, and $\sigma^3\tau$. That is, there are 5 subgroups of order 2.
3. Case $|H| = 4$: Groups of order 4 are either isomorphic to the cyclic group $\mathbb{Z}_4$, or the non-cyclic group $\langle \mathbb{Z}_8^*, \cdot \rangle$, where $\mathbb{Z}_8^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$. There are two elements in D_4 that have order 4. They are σ and σ^3. They generate the same subgroup $\langle \sigma \rangle$ of order 4. It remains to consider the subgroups that are isomorphic to $\mathbb{Z}_8^*$. We will continue on the next slide.
4. Case $|H| = 8$: We have $H = D_4$.

Applications

Note that a group isomorphic to $\mathbb{Z}_8^*$ can be written as $\{e, a, b, ab\}$ where $a^2 = b^2 = e$ and $ab = ba$. Thus, we are looking for two elements a and b of order 2 in D_4 that satisfies $ab = ba$. There are 5 elements of order 2. They are σ^2, τ, $\sigma\tau$, $\sigma^2\tau$, and $\sigma^3\tau$. Consider case by case. We find the following pairs (a, b) satisfy $ab = ba$: (σ^2, τ), $(\sigma^2, \sigma\tau)$, $(\sigma^2, \sigma^2\tau)$, $(\sigma^2, \sigma^3\tau)$, $(\tau, \sigma^2\tau)$, and $(\sigma\tau, \sigma^3\tau)$. The subgroups they generate are $\{e, \sigma^2, \tau, \sigma^2\tau\}$ and $\{e, \sigma^2, \sigma\tau, \sigma^3\tau\}$.

Conclusion. There are 10 subgroups in D_4. One has order 1, 5 has order 2, 1 is cyclic of order 4, two are non-cyclic of order 4, and one is D_4 itself. The subgroup diagram is given on Page 80.

Homework

Do Problems 4, 6, 12, 16, 28, 29, 32, 33, 35, 38, 39, 40 of Section 10.