Lecture 12

Reference: Judson, Chapter 6

Cosets and Lagrange's theorem

Left and right cosets

Recall the definition

Definition 1

Let G be a group and H a subgroup of G. A *left coset* of H is a subset of G of the form

$$gH = \{gh,\ h \in H\}.$$

In the same way, we can define **right** cosets to be $Hg = \{hg,\ h \in H\}$ for $g \in G$.

Proposition 1

Consider the relation

$$a \sim b \quad \text{if there exists } h \in H \text{ such that } a = bh.$$

Equivalently, $a \sim b$ if and only if $b^{-1}a \in H$ and if and only if $a \in bH$. It is an equivalence relation, and the left cosets of H are its equivalence classes.

Proof. To verify that equivalence classes modulo relation $\sim$ coincide with left cosets we need to verify two claims:

1. If $a \sim b$, i.e., $a^{-1}b \in H$, and a belongs to a coset gH, then b belongs the same coset. Indeed, since $a \sim b$, we have that there exists $h \in H$ such that $a = bh$. On the other hand, since $a \in gH$, there exists h_1 such that $a = gh_1$. Substituting a, we find

$$bh = gh_1 \iff b = g(h_1h^{-1})$$

Thus b belongs to the same coset gH, as claimed.

2. If a, b belong to a left coset gH, then we can find two elements $h_a, h_b \in H$ such that

$$gh_a = a \quad gh_b = b$$

But then $a^{-1}b = (h_a^{-1}g^{-1})(gh_b) = h_a^{-1}h_b \in H$. Thus by definition $a \sim b$.

□

By the previous remark, we have the following:

Proposition 2

Let H be a subgroup of a group G. Then G is the disjoint union of the left cosets of H. In other words, the left cosets of H form a partition of G.

Remark 1

This property is also true for right cosets. This can be seen by introducing another equivalence relation $\sim'$ given by $a \sim' b$ if and only if there exists $h \in H$ such that $a = hb$ (or, equivalently, $ab^{-1} \in H$, or $a \in Hb$). Its equivalence classes are the right cosets. Note moreover that $a \sim b$ if and only if $a^{-1} \sim' b^{-1}$, so that $aH = bH$ if and only if $Ha^{-1} = Hb^{-1}$.

There is a map

$$i : \{\text{left cosets of } H\} \to \{\text{right cosets of } H\}$$

given by $i\colon aH \mapsto Ha^{-1}$, well-defined and injective thanks to the previous remark. It is also surjective since for all $b \in G$, $\alpha(b^{-1}H) = Hb$. We may conclude the following:

Proposition 3

Let G be a group and H a subgroup of G. Then the number of left cosets of H is equal to the number of right cosets.

Index of a subgroup

Definition 2

Let H be a subgroup of a group G. The index of H in G, denoted by $[G:H]$, is defined to be the number of distinct left cosets of H in G. If this number is infinite, then we write $[G:H] = \infty$.

Remark 2

By proposition 3, this is the same as the number of distinct right cosets.

Example 1

The index of $\{0,3\}$ in $\mathbb{Z}_6$ is 3.
Question: what is the index of $\langle k \rangle$ for $k \in \mathbb{Z}_n$.

Example 2

Consider $G = \mathbb{Z}$ and $H = n\mathbb{Z}$. Observe that in this case, the equivalence relation $\sim$ is exactly the relation of congruence modulo n, the cosets being exactly

$$n\mathbb{Z},\ 1+n\mathbb{Z}, \dots,\ (n-1)+n\mathbb{Z}.$$

Thus, $[\mathbb{Z}:n\mathbb{Z}] = n$.
In particular, index $[G:H]$ might be finite even if G and H are infinite.

Note that in general, $[G:H]$ may be infinite. For example, a left coset of the trivial group in a group G is of the form $\{a\}$ for $a \in G$. Thus, if G is infinite, $[G:\{e\}]$ is infinite.

Remark 3

If H is a subgroup of index 1 in G, then $H = G$.

Example 3: Subgroups of index 2

An important special case is that of subgroups of index 2. Let G be a group and H a subgroup of G such that $[G:H] = 2$. This means that we have two left cosets, one of them being H itself, and the other being $G \setminus H$, which should be the equivalence class of all $g \in G \setminus H$, so that G is the disjoint union $G = H \sqcup gH$ for any $g \in G \setminus H$. In exactly the same manner, we have two right cosets, one of them being H, and the other being given by Hg where g is any element of $G \setminus H$. Therefore, for all $g \in G \setminus H$, we have

$$gH = G \setminus H = Hg.$$

On the other hand, for all $g \in H$, we have

$$gH = H = Hg.$$

Therefore, we observe that in this case, the right cosets and the left cosets of H are the same.

Problem 1: For the cyclic subgroups H_1 and H_2 of $(S_3, *)$ (the groups of symmetries of a triangle) generated by the rotation and the reflection respectively, find its cosets and index.

Lagrange's theorem

Proposition 4

Any two cosets aH and bH have the same number of elements.

Proof. We construct a bijection between aH and bH, which will prove that these two sets have the same number of elements.
Define a map
$$f: aH \to bH$$
by sending each element $g = ah \in aH$ to $bh = (ba^{-1})g \in bH$. This map is bijection, since it admits an inverse (given by an analogous left multiplication with ab^{-1}). □

Observing that the group G therefore is partitioned into $[G:H]$ subsets which all have $|H|$ elements, we have the following important *counting formula*:

Theorem 1: Counting formula

Let G be a finite group and H a subgroup of G. Then
$$|G| = [G:H]|H|.$$

This formula makes sense even if some of $|G|, [G:H]$ and $|H|$ are infinite. An important consequence of this is Lagrange's theorem:

Theorem 2: Lagrange

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

Proof. By counting formula we have
$$|G| = [G:H]|H|$$
Since $[G:H]$ is an integer, it implies that $|H|$ divides $|G|$. □

Corollary 1

Let G be a finite group. The order of any element of G divides the size of G.

Proof. Any element $a \in G$ generates a cyclic subgroup $\langle a \rangle \subset G$ of size $\mathrm{ord}(a)$. By the previous theorem, $\mathrm{ord}(a)$ divides $|G|$. □

Corollary 2

Let G be a finite group with order a prime number p. Then G is cyclic, and any $a \in G$ different from the identity element is a generator.

Remark 4

Corollary 2 implies that up to isomorphism, there is only one group of order a prime p, namely $\mathbb{Z}/p\mathbb{Z}$. Note that we already knew that all elements of $\mathbb{Z}/p\mathbb{Z}$ except 0 are generators.