Week 5

5.1 Cosets and The Theorem of Lagrange

Let G be a group, H a subgroup of G. We are interested in knowing how large H is relative to G.

We define a relation $\sim_L$ on G as follows:

$$a \sim_L b \text{ if and only if } b = ah \text{ for some } h \in H,$$

or equivalently:

$$a \sim_L b \text{ if and only if } a^{-1}b \in H.$$

Exercise: $\sim_L$ is an equivalence relation.

We may therefore partition G into a disjoint union of equivalence classes with respect to $\sim_L$. We call these equivalence classes the **left cosets** of H in G; each left coset of H has the form

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

We could likewise define a relation $\sim_R$ on G by

$$a \sim_R b \text{ if and only if } b = ha \text{ for some } h \in H,$$

or equivalently:

$$a \sim_R b \text{ if and only if } ba^{-1} \in H.$$

$\sim_R$ is also an equivalence relation, whose equivalence classes, which are subsets of the form

$$Hb = \{hb : h \in H\}, \quad b \in G,$$

are called the **right cosets** of H in G.

Definition. The number of left cosets of a subgroup H of G is called the **index** of H in G. It is denoted by:

$$[G : H]$$

Theorem 5.1.1 (Lagrange)**.** *Let G be a finite group. Let H be subgroup of G, then $|H|$ divides $|G|$. More precisely, $|G| = [G : H] \cdot |H|$.*

Proof. We already know that the left cosets of H partition G. That is:

$$G = a_1 H \sqcup a_2 H \sqcup \ldots \sqcup a_{[G:H]} H,$$

where $a_i H \cap a_j H = \emptyset$ if $i \neq j$. Hence, $|G| = \sum_{i=1}^{[G:H]} |a_i H|$. Note that one of the left cosets, say $a_1 H$, is equal to $H = eH$. The theorem follows if we show that the size of each left coset of H is equal to $|H|$.

For each left coset S of H, pick an element $a \in S$, and define a map $\psi : H \longrightarrow S$ as follows:

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

We want to show that ψ is bijective.

For any $s \in S$, by definition of a left coset (as an equivalence class) we have $s = ah$ for some $h \in H$. Hence, ψ is surjective. If $\psi(h') = ah' = ah = \psi(h)$ for some $h', h \in H$, then $h' = a^{-1}ah' = a^{-1}ah = h$. Hence, ψ is one-to-one.

So we have a bijection between two finite sets. Hence, $|S| = |H|$. □

Remark. As a consequence of the Theorem of Lagrange, we see that the numbers of left cosets and right cosets, if finite, are equal to each other; more generally, the set of left cosets has the same cardinality as the set of right cosets.

Corollary 5.1.2. *Let G be a finite group. The order of every element of G divides the order of G.*

Proof. Since G is finite, any element of $g \in G$ has finite order $|g|$. Since the order of the subgroup:

$$H = \langle g \rangle = \{e, g, g^2, \ldots, g^{|g|-1}\}$$

is equal to $|g|$, it follows from Lagrange's Theorem that $|g| = |H|$ divides $|G|$. □

Corollary 5.1.3. *If the order of a group G is prime, then G is a cyclic group.*

Proof. Let G be a group such that $p = |G|$ is a prime number. Since $p \geq 2$, there exists $a \in G \setminus \{e\}$. The above corollary them says that $|a| \mid p$. But $|a| \neq 1$, so we must have $|a| = p$. This means that $G = \langle a \rangle$. □

Corollary 5.1.4. *If a group G is finite, then for all $g \in G$ we have:*

$$g^{|G|} = e.$$

Proof. The previous corollary already says that $|g| \mid |G|$, i.e. $|G| = k \cdot |g|$. So $g^{|G|} = (g^{|g|})^k = e$. □

5.2 Examples of cosets

Example 5.2.1. Let $G = (\mathbb{Z}, +)$. Let:

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

The set H is a subgroup of G. The left cosets of H in G are as follows:

$$3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z},$$

where $i + 3\mathbb{Z} := \{i + 3k : k \in \mathbb{Z}\}$.

In general, for $n \in \mathbb{Z}$, the left cosets of $n\mathbb{Z}$ in $\mathbb{Z}$ are:

$$i + n\mathbb{Z}, \quad i = 0, 1, 2, \ldots, n - 1.$$

Example 5.2.2. Let $G = \mathrm{GL}(n, \mathbb{R})$. Let:

$$H = \mathrm{GL}^+(n, \mathbb{R}) := \{h \in G : \det h > 0\}.$$

(**Exercise:** H is a subgroup of G.)

Let:

$$s = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \in G$$

Note that $\det s = \det s^{-1} = -1$.

For any $g \in G$, either $\det g > 0$ or $\det g < 0$. If $\det g > 0$, then $g \in H$. If $\det g < 0$, we write:

$$g = (ss^{-1})g = s(s^{-1}g).$$

Since $\det s^{-1}g = (\det s^{-1})(\det g) > 0$, we have $s^{-1}g \in H$. So, $G = H \sqcup sH$, and $[G : H] = 2$. Notice that both G and H are infinite groups, but the index of H in G is finite.

Example 5.2.3. Let $G = \mathrm{GL}(n, \mathbb{R})$, $H = \mathrm{SL}(n, \mathbb{R})$. For each $x \in \mathbb{R}^\times$, let:

$$s_x = \begin{pmatrix} x & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \in G$$

Note that $\det s_x = x$.

For each $g \in G$, we have:

$$g = s_{\det g}(s_{\det g}^{-1} g) \in s_{\det g} H$$

Moreover, for distinct $x, y \in \mathbb{R}^\times$, we have:

$$\det(s_x^{-1} s_y) = y/x \neq 1.$$

This implies that $s_x^{-1} s_y \notin H$, hence $s_y H$ and $s_x H$ are disjoint cosets. We have therefore:

$$G = \bigsqcup_{x \in \mathbb{R}^\times} s_x H.$$

The index $[G : H]$ in this case is infinite.

Exercise: For the subgroup $(\mathbb{Z}, +) < (\mathbb{R}, +)$, show that the set of (left) cosets are parametrized by $[0, 1)$, so that we have

$$\mathbb{R} = \bigsqcup_{t \in [0,1)} (t + \mathbb{Z}).$$

Exercise: For a vector subspace $W \subset V$, we consider the subgroup $(W, +) < (V, +)$. Then the set of cosets are given by the *affine translates* $v + W$, $v \in V$, of W in V. Let $W' \subset V$ be a subspace complementary to W, meaning that it satisfies the following conditions:

- $\dim W' = \dim V - \dim W$, and
- $W \cap W' = \{0\}$.

Show that the set of cosets of W in V are parametrized by W', so that

$$V = \bigsqcup_{v \in W'} (v + W).$$

Example 5.2.4. Consider the dihedral group D_n, and the cyclic subgroup $\langle r \rangle$ generated by the anticlockwise rotation by $2\pi/n$. Since

$$D_n = \{\text{id}, r, r^2, \ldots, r^{n-1}, s, rs, r^2 s, \ldots, r^{n-1} s\},$$

we directly see that

$$D_n = \langle r \rangle \sqcup s\langle r \rangle.$$

Example 5.2.5. Consider the n-th symmetric group S_n, and the subgroup $A_n < S_n$ consisting of all the even permutations. Let $\tau \in S_n$ be a transposition. **Exercise:** the map $\sigma \mapsto \tau\sigma$ gives a bijection between A_n and $B_n := S_n \setminus A_n$, the set of all odd permutations. Hence we have $S_n = A_n \sqcup \tau A_n$.

Example 5.2.6. Recall that $S_3 (= D_3)$ is generated by $\rho = (123)$ and $\mu = (12)$. (In fact, $S_3 = \{\text{id}, \rho, \rho^2, \mu, \rho\mu, \rho^2\mu\}$.) For the cyclic subgroup $H = \langle \mu \rangle < S_3$, the left cosets are given by $H, \rho H, \rho^2 H$ so that we have $S_3 = H \sqcup \rho H \sqcup \rho^2 H$.

5.3 Group Homomorphisms

Definition. Let $G = (G, *)$, $G' = (G', *')$ be groups.

A **group homomorphism** ϕ from G to G' is a map $\phi : G \longrightarrow G'$ which satisfies:

$$\phi(a * b) = \phi(a) *' \phi(b),$$

for all $a, b \in G$.

If ϕ is also bijective, then ϕ is called an **isomorphism**. If there exists an isomorphism $\phi : G \longrightarrow G'$ between two groups G and G', then we say G is **isomorphic** to G', and denoted by $G \simeq G'$.

Remark. Note that if a homomorphism ϕ is bijective, then $\phi^{-1} : G' \longrightarrow G$ is also a homomorphism, and consequently, ϕ^{-1} is an isomorphism.

Isomorphic groups have the same algebraic structure and thus share the same algebraic properties – they only differ by relabeling of their elements. One of the most fundamental questions in group theory is to classify groups up to isomorphisms.

Example 5.3.1.

- Let V, W be vector spaces over $\mathbb{R}$ (or $\mathbb{C}$). Then a linear transformation $\phi : V \longrightarrow W$ is in particular a homomorphism between abelian groups $\phi : (V, +) \longrightarrow (W, +)$.
- The determinant $\det : \mathrm{GL}(n, \mathbb{R}) \longrightarrow \mathbb{R}^\times$ is a group homomorphism.
- The exponential map $\exp : (\mathbb{R}, +) \longrightarrow (\mathbb{R}_{>0}, \cdot)$ is an isomorphism from the additive group of real numbers to the multiplicative group of positive real numbers, whose inverse if given by the logarithm $\log : (\mathbb{R}_{>0}, \cdot) \longrightarrow (\mathbb{R}, +)$.