Queen Mary University of London

MTH4104 **Introduction to Algebra**

Cosets and Lagrange's theorem **Spring 2021**

In Section 7.6 of the lecture notes, we saw that $4\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. Now $\mathbb{Z}$ can be partitioned into four congruence classes mod 4, one of which is the subgroup $4\mathbb{Z}$. We now generalise this to any group and any subgroup.

Let G be a group and H a subgroup of G. Define a relation $\sim$ on G by

$$g_1 \sim g_2 \text{ if and only if } g_2 \diamond g_1^{-1} \in H.$$

We claim that $\sim$ is an equivalence relation.

reflexive: $g_1 \diamond g_1^{-1} = e \in H$, so $g_1 \sim g_1$.

symmetric: Let $g_1 \sim g_2$, so that $h = g_2 \diamond g_1^{-1} \in H$. Then $h^{-1} = g_1 \diamond g_2^{-1} \in H$, so $g_2 \sim g_1$.

transitive: Suppose that $g_1 \sim g_2$ and $g_2 \sim g_3$. Then $h = g_2 \diamond g_1^{-1} \in H$ and $k = g_3 \diamond g_2^{-1} \in H$. Then

$$k \diamond h = (g_3 \diamond g_2^{-1}) \diamond (g_2 \diamond g_1^{-1}) = g_3 \diamond g_1^{-1} \in H,$$

so $g_1 \sim g_3$.

Now since we have an equivalence relation on G, the set G is partitioned into equivalence classes for the relation. These equivalence classes are called *cosets* of H in G, and the number of equivalence classes is the *index* of H in G, written $|G : H|$.

What do cosets look like?

For any $g \in G$, let

$$H \diamond g = \{h \diamond g : h \in H\}.$$

We claim that any coset has this form. Take $g \in G$, and let X be the equivalence class of $\sim$ containing g. That is, $X = \{x \in G; g \sim x\}$.

- Take $x \in X$. Then $g \sim x$, so $x \diamond g^{-1} \in H$. Let $h = x \diamond g^{-1}$. Then $x = h \diamond g \in H \diamond g$.
- Take an element of $H \diamond g$, say $h \diamond g$. Then $(h \diamond g) \diamond g^{-1} = h \in H$, so $g \sim h \diamond g$; thus $h \diamond g \in X$.

So every equivalence class is of the form $H \diamond g$. We have shown:

Theorem 0.1. *Let H be a subgroup of G. Then the cosets of H in G are the sets of the form*

$$H \diamond g = \{h \diamond g : h \in H\}$$

and they form a partition of G.

Example Let $G = \mathbb{Z}$ and $H = 4\mathbb{Z}$. Since the group operation is $+$, the cosets of H are the sets $H + a$ for $a \in G$, that is, the congruence classes. There are four of them, so $|G : H| = 4$.

Remark. We write the coset as $H \diamond g$, and call the element g the *coset representative*. But **any** element of the coset can be used as its representative. In the above example,

$$4\mathbb{Z} + 1 = 4\mathbb{Z} + 5 = 4\mathbb{Z} - 7 = 4\mathbb{Z} + 100001 = \cdots$$

If G is finite, the *order* of G is the number of elements of G. (If G is infinite, we sometimes say that it has infinite order.) We write the order of G as $|G|$.

Now the partition into cosets allows us to prove an important result, *Lagrange's Theorem*:

Theorem 0.2. *Let G be a finite group, and H a subgroup of G. Then $|H|$ divides $|G|$. In fact, $|G| = |G : H| \cdot |H|$, where $|G : H|$ is the index of H in G.*

Proof. We know that G is partitioned into exactly $|G : H|$ cosets of H. If we can show that each coset has the same number as elements as H does, then the theorem will be proved.

So let $H \diamond g$ be a coset of H. We define a function $f : H \to H \diamond g$ by the rule that $f(h) = h \diamond g$. We show that f is one-to-one and onto. Then the conclusion that $|H \diamond g| = |H|$ will follow.

f is one-to-one: suppose that $f(h_1) = f(h_2)$, that is, $h_1 \diamond g = h_2 \diamond g$. By the Cancellation Law, $h_1 = h_2$.

f is onto: take an element $x \in H \diamond g$, say $x = h \diamond g$. Then $x = f(h)$, as required. □