7. Cosets

Consider the group of integers $\mathbb{Z}$ under addition. Let H be the subgroup of even integers. Notice that if you take the elements of H and add one, then you get all the odd elements of $\mathbb{Z}$. In fact if you take the elements of H and add any odd integer, then you get all the odd elements.

On the other hand, every element of $\mathbb{Z}$ is either odd or even, and certainly not both (by convention zero is even and not odd), that is, we can partition the elements of $\mathbb{Z}$ into two sets, the evens and the odds, and one part of this partition is equal to the original subset H.

Somewhat surprisingly, this rather trivial example generalises to the case of an arbtirary group G and subgroup H and in the case of finite groups imposes rather strong conditions on the size of a subgroup.

To go further, we need to recall some basic facts about partitions and equivalence relations.

Definition 7.1. *Let X be a set. An* ***equivalence relation*** $\sim$ *is a relation on X, which is*

reflexive: *For every $x \in X$, $x \sim x$.*
symmetric: *For every x and $y \in X$, if $x \sim y$ then $y \sim x$.*
transitive: *For every x and y and $z \in X$, if $x \sim y$ and $y \sim z$ then $x \sim z$.*

Lemma 7.2. *Let G be a group and let H be a subgroup. Let $\sim$ be the relation on G defined by the rule*

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

Then $\sim$ is an equivalence relation.

Proof. There are three things to check.

First we check reflexivity. Suppose that $a \in G$. Then $a^{-1}a = e \in H$, since H is a subgroup. But then $a \sim a$ by definition of $\sim$ and $\sim$ is reflexive.

Now we check symmetry. Suppose that a and b are elements of G and that $a \sim b$. Then $b^{-1}a \in H$. As H is closed under taking inverses, $(b^{-1}a)^{-1} \in H$. But

$$\begin{aligned}(b^{-1}a)^{-1} &= a^{-1}(b^{-1})^{-1} \\ &= a^{-1}b.\end{aligned}$$

Thus $a^{-1}b \in H$. But then by definition $b \sim a$. Thus $\sim$ is symmetric.

Finally we check transitivity. Suppose that $a \sim b$ and $b \sim c$. Then $b^{-1}a \in H$ and $c^{-1}b \in H$. As H is closed under multiplication

$(c^{-1}b)(b^{-1}a) \in H$. On the other hand

$$\begin{aligned}(c^{-1}b)(b^{-1}a) &= c^{-1}(bb^{-1})a \\ &= c^{-1}(ea) \\ &= c^{-1}a.\end{aligned}$$

Thus $c^{-1}a \in H$. But then $a \sim c$ and $\sim$ is transitive.

As $\sim$ is reflexive, symmetric and transitive, it is an equivalence relation. □

On the other hand if we are given an equivalence relation, the natural thing to do is to look at its equivalence classes.

Definition 7.3. *Let $\sim$ be an equivalence relation on a set X. Let $a \in X$ be an element of X. The* ***equivalence class*** *of a is*

$$[a] = \{\, b \in X \mid b \sim a \,\}.$$

Definition 7.4. *Let X be a set. A* ***partition*** *P of X is a collection of non-empty subsets A_i, $i \in I$, such that*

(1) The A_i cover X, that is

$$\bigcup_{i \in I} A_i = X.$$

(2) The A_i are pairwise disjoint, that is, if $i \neq j$ then

$$A_i \cap A_j = \emptyset.$$

Lemma 7.5. *Given an equivalence relation $\sim$ on X there is a unique partition of X. The elements of the partition are the equivalence classes of $\sim$ and vice-versa. That is, given a partition P of X we may construct an equivalence relation $\sim$ on X such that the partition associated to $\sim$ is precisely P.*

Concisely, the data of an equivalence relation is the same as the data of a partition.

Proof. Suppose that $\sim$ is an equivalence relation. Note that $x \in [x]$ as $x \sim x$. Thus certainly the set of equivalence classes covers X. The only thing to check is that if two equivalence classes intersect at all, then in fact they are equal.

We first prove a weaker result. We prove that if $x \sim y$ then $[x] = [y]$. Since $y \sim x$, by symmetry, it suffices to prove that $[x] \subset [y]$. Suppose that $a \in [x]$. Then $a \sim x$. As $x \sim y$ it follows that $a \sim y$, by transitivity. But then $a \in [y]$. Thus $[x] \subset [y]$ and by symmetry $[x] = [y]$.

So suppose that $x \in X$ and $y \in X$ and that $z \in [x] \cap [y]$. As $z \in [x]$, $z \sim x$. As $z \in [y]$, $z \sim y$. But then by what we just proved $[x] = [z] = [y]$.

Thus if two equivalence classes overlap, then they coincide and we have a partition.

Now suppose that we have a partition

$$P = \{ A_i \mid i \in I \}.$$

Define a relation $\sim$ on X by the rule that $x \sim y$ if and only if $x \in A_i$ and $y \in A_i$ (same i of course). That is, x and y are related if and only if they belong to the same part. It is straightforward to check that this is an equivalence relation, and that this process reverses the one above. Both of these things are left as an exercise to the reader. □

Example 7.6. *Let X be the set of integers.*

Define an equivalence relation on $\mathbb{Z}$ by the rule $x \sim y$ if and only if $x - y$ is even.

Then the equivalence classes of this relation are the even and odd numbers.

More generally, let n be an integer, and let $n\mathbb{Z}$ be the subset consisting of all multiples of n,

$$n\mathbb{Z} = \{ an \mid a \in \mathbb{Z} \}.$$

Since the sum of two multiples of n is a multiple of n,

$$an + bn = (a + b)n$$

and the inverse of a multiple of n is a multiple of n,

$$-(an) = (-a)n,$$

$n\mathbb{Z}$ is closed under multiplication and inverses. Thus $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

The equivalence relation corresponding to $n\mathbb{Z}$ becomes $a \sim b$ if and only if $a-b \in n\mathbb{Z}$ that is $a-b$ is a multiple of n. There are n equivalence classes,

$$[0], [1], [2], [3], \dots [n - 1].$$

Definition-Lemma 7.7. *Let G be a group and let H be a subgroup. Let $g \in G$. Then*

$$[g] = gH = \{ gh \mid h \in H \}.$$

*gH is called a **left coset** of H.*

Proof. Suppose that $k \in [g]$. Then $k \sim g$ and so $g^{-1}k \in H$. So if we set $h = g^{-1}k$, then $h \in H$. But then $k = gh \in gH$. Thus $[g] \subset gH$.

Now suppose that $k \in gH$. Then $k = gh$ for some $h \in H$. But then $h = g^{-1}k \in H$. By definition of $\sim$, $k \sim g$. But then $k \in [g]$. $\square$

In the example above, we see that the left cosets are

$$\begin{aligned}
[0] &= \{\, an \mid a \in \mathbb{Z} \,\} \\
[1] &= \{\, an + 1 \mid a \in \mathbb{Z} \,\} \\
[2] &= \{\, an + 2 \mid a \in \mathbb{Z} \,\} \\
&\vdots \\
[n-1] &= \{\, an - 1 \mid a \in \mathbb{Z} \,\}.
\end{aligned}$$

It is interesting to see what happens in the case $G = D_3$. Suppose we take $H = \{I, R, R^2\}$. Then

$$[I] = H = \{I, R, R^2\}.$$

Pick $F_1 \notin H$. Then

$$[F_1] = F_1H = \{F_1, F_2, F_3\}.$$

Thus H partitions G into two sets, the rotations, and the flips,

$$\{\{I, R, R^2\}, \{F_1, F_2, F_3\}\}.$$

Note that both sets have the same size.

Now suppose that we take $H = \{I, F_1\}$ (up to the obvious symmetries, this is the only other interesting example).

In this case

$$[I] = IH = H = \{I, F_1\}.$$

Now R is not in this equivalence class, so

$$[R] = RH = \{R, RF_1\} = \{R, F_2\}.$$

Finally look at the equivalence class containing R^2.

$$[R^2] = R^2H = \{R^2, R^2F_1\} = \{R, F_3\}.$$

The corresponding partition is

$$\{\{I, F_1\}, \{R, F_2\}, \{R^2, F_3\}\}.$$

Note than once again, each part of the partition has the same size.