MTH101: Symmetry

Tutorial 03

Problem 1. In the group of symmetries of the regular n-gon, denoted by D_n, let ρ denote the rotation through $2\pi/n$ radians and let τ denote one of the reflections. Then, we know that $\rho^n = 1$, $\tau^2 = 1$ and $\rho\tau = \tau\rho^{-1}$. Let H denote the group $\{1, \rho^2\tau\}$. (Check that this really is a subgroup of D_n.) Describe all the left and right cosets of H.

Solution. Elements of D_n are of two types:

- Rotations of the form ρ^i for $0 \leqslant i \leqslant n-1$, and
- Reflections of the form $\rho^i\tau$ for $0 \leqslant i \leqslant n-1$.

For any i, $0 \leqslant i \leqslant n-1$, the left coset $\rho^i H$ is the set

$$\{\rho^i, \rho^i \cdot \rho^2\tau\} = \{\rho^i, \rho^{i+2}\tau\}.$$

These are actually *all* the left cosets since we expect to get only n distinct left cosets anyway. (The number of cosets is equal to the order of the group divided by the order of the subgroup. So in this case, we expect to find $2n/n = n$ distinct cosets.) However, to see this explicitly, we note that for any reflection $\rho^j\tau$, the coset $\rho^j\tau H$ is the set

$$\{\rho^j\tau, \rho^j\tau\rho^2\tau\} = \{\rho^j\tau, \rho^{j-2}\} = \rho^{j-2}H.$$

Now, let us look at the right cosets. For any i, $0 \leqslant i \leqslant n-1$, the right coset $H\rho^i$ is the set

$$\{\rho^i, \rho^2\tau\rho^i\} = \{\rho^i, \rho^{-i+2}\tau\}.$$

Just as we argued above, these are actually *all* the right cosets since we expect to get only n distinct right cosets anyway. Again, to see this explicitly, we note that for any reflection $\rho^j\tau$, the coset $H\rho^j\tau$ is the set

$$\{\rho^j\tau, \rho^2\tau\rho^j\tau\} = \{\rho^j\tau, \rho^{-j+2}\} = \rho^{-(j-2)}H.$$

$\square$

Problem 2. Let G be a group such that $ord(x) \leqslant 2$ for any $x \in G$. Prove that $xy = yx$ for any $x, y \in G$. (In other words, G is an *abelian* group.)

Proof. Since every element z of G has order 1 or 2, we see that $z^2 = 1$. Thus, $z = z^{-1}$ for every element z of G.

Now, let x and y be elements of G. We want to prove $xy = yx$. As we saw above, $x^{-1} = x$ and $y^{-1} = y$. Thus, $(xy)^{-1} = y^{-1}x^{-1} = yx$. However, by applying the above observation to the element xy, we also see that $(xy)^{-1} = xy$. Thus, we see that $xy = yx$. $\square$

Problem 3. Let S be a set and let $G = Perm(S)$. Let us fix an element x of S. Let $H = \{\sigma \in Perm(S) | \sigma(x) = x\}$. Prove that $\sigma, \tau \in G$ are in the same left coset of H if and only if $\sigma(x) = \tau(x)$. Can you formulate and prove a similar statement for right cosets?

Solution. First, let us confirm that H is actually a subgroup of G. (The problem does not ask you to check this, but let us do it anyway.)

It is clear that the identity morphism id is an element of H since $id(x) = x$. Also, if $\sigma, \tau \in H$, then $\sigma(x) = x$ and $\tau(x) = x$. Thus, $\sigma \circ \tau(x) = \sigma(\tau(x)) = \sigma(x) = x$. This shows that H is closed under the binary operation on G (which is just composition of functions). Also, if $\sigma \in H$, then $\sigma(x) = x$ and so $\sigma^{-1}(x) = x$. Thus, $\sigma^{-1} \in H$. Thus, we see that H is a subgroup of G.

Now, suppose σ and τ are elements of G such that $\sigma(x) = \tau(x)$. Then $\tau^{-1}(\sigma(x)) = \tau^{-1}(\tau(x)) = x$. Thus, $\tau^{-1} \circ \sigma(x) = x$, i.e. $\tau^{-1} \circ \sigma \in H$. Thus, there exists an element $\phi \in H$ such that $\tau^{-1} \circ \sigma = \phi$, i.e. $\sigma = \tau \circ h$. Thus, $\sigma \in \tau H$. This shows that σH and τH are not disjoint, i.e. $\sigma H = \tau H$.

Conversely, suppose that σ and τ are in the same left coset of H. Then, $\sigma H = \tau H$. Thus, $\sigma \in \tau H$. Thus, there exists an element $\phi \in H$ such that $\sigma = \tau\phi$. Thus, $\sigma(x) = \tau(\phi(x))$. But, as $\phi \in H$, $\phi(x) = x$. Thus, $\sigma(x) = \tau(\phi(x)) = \tau(x)$. This completes the proof of the required statement about left cosets.

Now, let us see if we can formulate a similar characterization of right cosets.

Suppose $\sigma, \tau \in G$ are such that $H\sigma = H\tau$. Thus, $\sigma = \phi\tau$ for some $\phi \in H$. Thus, if y is an element of S such that $\tau(y) = x$, then $\sigma(y) = \phi(\tau(y)) = \phi(x) = x$. Thus, we see that σ and τ map the same element of S to x. In other words, $\sigma^{-1}(x) = \tau^{-1}(x)$.

Conversely, suppose $\sigma, \tau \in G$ are such that $\sigma^{-1}(x) = \tau^{-1}(x)$. Then,

$$x = \sigma(\sigma^{-1}(x)) = \sigma(\tau^{-1}(x)) = \sigma \circ \tau^{-1}(x).$$

In other words, $\sigma \circ \tau^{-1} \in H$. Thus, there exists an element $\phi \in H$ such that $\sigma \circ \tau^{-1} = \phi$. Thus, $\sigma = \phi \circ \tau$ and so $\sigma \in H\tau$. Thus, the right cosets $H\sigma$ and $H\tau$ are not disjoint, i.e. $H\sigma = H\tau$.

Thus, we have proved that σ and τ lie in the same right coset of H if and only if $\sigma^{-1}(x) = \tau^{-1}(x)$. ☐

Problem 4. Let $S = \{1, 2, 3, 4, 5, 6, 7\}$. Let $G = Perm(S)$. Find an element $\sigma \in G$ such that $ord(\sigma) = 12$.

Solution. (This problem was intended as an early introduction to some ideas that will be explored in detail in later lectures.)

Suppose σ is any element of $Perm(S)$. Let x be any element of S. Then the sequence $x, \sigma(x), \sigma^2(x), \ldots$ must have some repetitions. Suppose $\sigma^i(x) = \sigma^j(x)$ for non-negative integers i, j such that $i < j$. Then, $x = \sigma^{-i} \circ \sigma^j(x)$. Thus, $x = \sigma^{j-i}(x)$. Thus, we see that x itself must appear again in this sequence, i.e. there exists a *positive* integer k such that $\sigma^k(x) = x$. Choose m_1 to be the *smallest* positive integer such that $\sigma^{m_1}(x) = x$.

Thus, the sequence $x, \sigma(x), \sigma^2(x), \ldots$ repeats after m_1 steps. In fact, we can also see that the m_1 elements $x, \sigma(x), \ldots, \sigma^{m_1-1}(x)$ are all distinct. Indeed, if $\sigma^i(x) = \sigma^j(x)$ for some i and j such that $0 \leqslant i < j \leqslant m_1 - 1$, then $\sigma^{j-i}(x) = x$, but $j - i < m_1$, which contradicts our choice of m_1. Thus, σ permutes the m_1 distinct elements $\{x, \sigma(x), \ldots, \sigma^{m_1-1}(x)\}$ in a cycle. Let us denote this set $\{x, \sigma(x), \ldots, \sigma^{m_1-1}(x)\}$ by A_1.

Now, S has more than m elements, we pick some element y which is not in the set $\{x, \sigma(x), \cdot, \sigma^{m_1-1}(x)\}$ and repeat the argument for the sequence $y, \sigma(y), \sigma^2(y), \ldots$ instead. This will give us another collection of elements $A_2 = \{y, \sigma(y), \ldots, \sigma^{m_2}(y)\}$ (for some integer m_2), the elements of which are permuted in a cycle by σ.

We keep repeating this process, until we run out of elements of S. Thus, we get a partitioning of S into disjoint sets $A_1, \ldots, A_r$ each of which is permuted cyclically by σ. Suppose the sizes of these sets are $m_1, \ldots, m_r$. The action of σ on A_i is cyclic with period m_i. Thus, the order of σ as an element of $Perm(S)$ is the least common multiple of $m_1, \ldots, m_r$.

Thus, if we can build a permutation σ which divides S into two cycles of size 3 and 4, then the order of σ will be 12. One such example is given by defining σ as follows: $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 1$, $\sigma(4) = 5$, $\sigma(5) = 6$, $\sigma(6) = 7$, $\sigma(7) = 4$. ☐