# MTH 301 Quiz 1 Solutions

1. Let G be a finite group, and let $H, K \leq G$. Using the orbit-stabilizer theorem establish that

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

**Solution.** Consider the map

$$(H \times K) \times G \xrightarrow{\varphi} G : ((h,k), g) \overset{\varphi}{\mapsto} (h,k) \cdot g = hgk^{-1}.$$

We claim that this map indeed defines an action $H \times K \curvearrowright G$. First, we note that from the basic group axioms in $G$, it follows that $\varphi$ is a well-defined function (Verify this!). Now, if we consider the identity $(1,1) \in H \times K$, we see that

$$(1,1) \cdot g = \varphi((1,1), g) = 1 \cdot g \cdot 1 = g, \ \forall g \in G.$$

Furthermore, we have

$$\begin{aligned} (h_1, k_1) \cdot ((h_2, k_2) \cdot g)) &= \varphi((h_1, k_1), \varphi((h_2, k_2), g)) \\ &= h_1(h_2 g k_2^{-1}) k_1^{-1} \\ &= (h_1 h_2) g (k_1 k_2)^{-1} \\ &= (h_1 h_2, k_1 k_2) \cdot g, \end{aligned}$$

which shows that $\varphi$ defines an action $H \times K \curvearrowright G$.

Under this action, we see that

$$\mathcal{O}_1 = \{hk^{-1} : (h,k) \in H \times K\} = HK,$$

which shows that

$$|\mathcal{O}_1| = |HK|. \tag{1}$$

(Can you determine what is $\mathcal{O}_g$ when $g \neq 1$?)

Furthermore, the stabilizer of 1 under this action is given by

$$\begin{aligned} (H \times K)_1 &= \{(h,k) \in H \times K : (h,k) \cdot 1 = 1\} \\ &= \{(h,k) \in H \times K : hk^{-1} = 1\} \\ &= \{(h,k) \in H \times K : h = k\} \\ &= H \cap K, \end{aligned}$$

from which it follows that

$$|(H \times K)_1| = |H \cap K|. \tag{2}$$

(Can you determine what is $(H \times K)_g$ when $g \neq 1$?)
From the Orbit-Stabilizer theorem, we have that

$$|\mathcal{O}_1| = \frac{|H \times K|}{|(H \times K)_1|}. \tag{3}$$

The assertion now follows by substituting the appropriate values from (1) and (2) in (3).

2. Consider the action of the matrix group

$$\mathrm{GL}(2,\mathbb{Z}) = \{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{Z} \text{ and } ad - bc = \pm 1\}$$

on $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$ defined by

$$\mathrm{GL}(2,\mathbb{Z}) \times \mathbb{Z}^2 \to \mathbb{Z}^2 : (\begin{bmatrix} a & b \\ c & d \end{bmatrix}, (z_1, z_2)) \mapsto (az_1 + bz_2, cz_1 + dz_2).$$

Show that each orbit comprises the elements in $\mathbb{Z}^2$ whose coordinates have a fixed greatest common divisor.

**Solution.** If $d = \gcd(z_1, z_2)$, then by the Bezout's identity, there exists $p, q \in \mathbb{Z}$ such that $pz_1 + qz_2 = d$. Moreover, since $d \mid z_i$, we have

$$\begin{bmatrix} p & q \\ -z_2/d & z_1/d \end{bmatrix} \in \mathrm{GL}(2,\mathbb{Z}) \text{ and } \begin{bmatrix} p & q \\ -z_2/d & z_1/d \end{bmatrix} \cdot (z_1, z_2) = (d, 0).$$

By a similar argument, for any $(w_1, w_2) \in \mathbb{Z}^2$ such that $d = \gcd(w_1, w_2)$, there exists integers $p', q'$ and a matrix

$$\begin{bmatrix} p' & q' \\ -w_2/d & w_1/d \end{bmatrix} \in \mathrm{GL}(2,\mathbb{Z}) \text{ such that } \begin{bmatrix} p' & q' \\ -w_2/d & w_1/d \end{bmatrix} \cdot (w_1, w_2) = (d, 0).$$

So, it follows that

$$\begin{bmatrix} p' & q' \\ -w_2/d & w_1/d \end{bmatrix}^{-1} \begin{bmatrix} p & q \\ -z_2/d & z_1/d \end{bmatrix} \cdot (z_1, z_2) = (w_1, w_2).$$

Therefore, if $\gcd(z_1, z_2) = \gcd(w_1, w_2)$, then $(z_1, z_2)$ and $(w_1, w_2)$ are in the same orbit under the action.

Conversely, suppose that $(z_1, z_2)$ and $(w_1, w_2)$ are in the same orbit under the action. Then there exists

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}(2, \mathbb{Z}) \text{ such that } \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot (z_1, z_2) = (w_1, w_2).$$

So, it follows that

$$az_1 + bz_2 = w_1 \text{ and } cz_1 + dz_2 = w_2.$$

From the Bezout's identity, it follows that $\gcd(z_1, z_2) \mid w_1$ and $\gcd(z_1, z_2) \mid w_2$, and hence we have:

$$\gcd(z_1, z_2) \mid \gcd(w_1, w_2). \text{ (Why?)} \tag{4}$$

By switching the roles of $(z_1, z_2)$ and $(w_1, w_2)$ and following an analogous argument, we can conclude that

$$\gcd(w_1, w_2) \mid \gcd(z_1, z_2). \tag{5}$$

Thus, from (4) and (5), it follows that $\gcd(w_1, w_2) = \gcd(z_1, z_2)$.