Math 171

Quiz 3

Solve the following. Your solutions must be neatly presented and all statements must be justified.

1. Find all subgroups of $\mathbb{Z}_{41}$. (Fun fact: 41 is prime.)

   Solution: Write $\mathbb{Z}_{41}$ as $\{[0], [1], \ldots, [40]\}$. Let H be any non-trivial subgroup. Then there exists $[k] \in H$ such that $[k] \neq [0]$. Hence we may choose k such that $0 < k < 41$. Since 41 is prime, $\gcd(k, 41) = 1$. Hence $[k]$ is a generator of $\mathbb{Z}_{41}$ and therefore $H = \mathbb{Z}_{41}$. Hence the only two subgroups are $\{[0]\}$ and $\mathbb{Z}_{41}$.

2. Prove or give a counter-example:

   (a) If G is a cyclic group with 3 generators then G is a finite group.

   Solution: True. If G is not finite then G is an infinite cyclic group. Therefore G is isomorphic to $\mathbb{Z}$. The only generators of $\mathbb{Z}$ are $\{-1, 1\}$. Hence contradiction.

   (b) If G is a finite group such that every proper subgroup of G is cyclic, then G is cyclic.

   Solution: False. Consider the Klein 4 group: $V = \{e, a, b, c\}$ whose multiplication table is:

$$\begin{array}{ccc} aa = e & ab = c & ac = b \\ ba = c & bb = e & bc = a \\ ca = b & cb = a & cc = e \end{array}$$

   (Here e is the identity element.) Observe that if H is any subgroup containing more than 2 elements it must be the entire group, and hence not proper. The square of any element is the identity, therefore we have subgroups containing 2 elements and hence are isomorphic to $\mathbb{Z}_2$ (hence cyclic). A subgroup with 1 element is, of course, the trivial subgroup which is the cyclic group generated by e. Hence every proper subgroup of V is cyclic. But V itself is not cyclic since it does not contain an element of order 4.

3. Consider the following element of S_6:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 3 & 1 & 5 & 2 \end{pmatrix}.$$

   Find σ^n for all **odd** integers n.

   Solution: Observe that $\sigma^2 = \mathrm{id}$, where id is the identity permutation. Let $n = 2k+1$. Then $\sigma^n = \sigma^{2k} \circ \sigma = \mathrm{id} \circ \sigma = \sigma$.