Homework Assignment # 5 - Solutions

1. Find all the generators of $Z_6, Z_8,$ and Z_{20}.

   Solution:

   $Z_6 = \langle 1 \rangle = \langle 5 \rangle$

   $Z_8 = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle$

   $Z_{20} = \langle 1 \rangle = \langle 3 \rangle = \langle 7 \rangle = \langle 9 \rangle = \langle 11 \rangle = \langle 13 \rangle = \langle 17 \rangle = \langle 19 \rangle$

   Notice that the group is generated by elements relatively prime to n!

QED

2. Suppose that a cyclic group G has exactly three subgroups: G itself, $\{e\}$, and a subgroup of order 7. What is $|G|$? What can you say if 7 were replaced by p, where p is a prime?

   Solution:

   (a)

   First, note that G is not infinite since an infinite cyclic group has infinitely many subgroups. Now, since G has exactly 3 subgroups of orders 7, 1, and 7 respectively and the divisors of 49 are 1, 7, and 49, clearly $|G| = 7^2 = 49$.

   As a check, you can see that we have the trivial subgroup, a subgroup of order 7, and the entire group itself (order 49).

   (b)

   In general, $|G| = p^2$ (Examine the pattern in part (a)).

QED

3. Prove that Z_n has an even number of generators if $n > 2$.

Proof:

If g a generator of z_n, then $\{g^k \mid k \in Z\} = G$. Clearly, $g^{-1} = -g$ is also a generator for Z_n. So, for any $g \in G$ such that $G = \langle g \rangle$, $G = \langle g^{-1} \rangle$ as well. So, we conclude that non-trivial generators come in pairs. We note that the identity is the only generator such that $g^2 = e$ (i.e. its own inverse) since if $g \neq e$, we have $g^{-1} = -g = n - g$. Thus, for $n > 2$, Z_n has an even number of generators.

QED

4. Show $Z_{2^{2002}}$ has no subgroup of order 3^k for any $k \geq 1$.

Proof:

$\left|Z_{2^{2002}}\right| = 2^{2002}$. Now if H a subgroup of $Z_{2^{2002}}$, then $|H|$ divides 2^{2002}. But, 3^k does not divide 2^{2002} $\forall\, k$ since 2 and 3 are distinct primes (i.e. Fund. thm. of arithmatic.).

Thus, there exists no subgroup of order 3^k for any k.

5. Let $H = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \mid n \in Z \right\}$. Show that H is a cyclic subgroup of $GL(2, R)$.

(Hint: You must first show that H is a subgroup and then show H cyclic.)

Proof:

Take $x, y \in H$. Then, $x = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$, $y = \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix}$, and $m, n \in Z$. Now,

$xy^{-1} = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -m \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & n-m \\ 0 & 1 \end{bmatrix}$. Since $n - m \in Z$, we see that $xy^{-1} \in H$. Thus H a subgroup of $GL(2, R)$.

5. (Cont.)

Proof (Cont.):

Now, to show that H is cyclic, notice that $H = \left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle$, since $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$.

So, H is a cyclic subgroup of $GL(2, R)$.