Problem Set 2 - Solutions

1. Let x and y be elements of order 2 in any group. Prove that if $t = xy$ then $tx = xt^{-1}$.

   Proof: Suppose $x, y \in G, |x| = |y| = 2$, and $t = xy$. Thus $x^2 = e,\ y^2 = e,$ and x,y $\neq$ e (By Def.). In other words, x and y are their own inverses. Now,

   $tx = xyx = xy^{-1}x^{-1} = x\left(y^{-1}x^{-1}\right) = x\left(xy\right)^{-1} = xt^{-1}$ QED

2. Suppose $G = \langle a \rangle$. Show $G = \langle a^{-1} \rangle$.

   Proof: By definition, $G = \langle a \rangle$ implies that $G = \left\{a^n \mid a \in Z\right\}$. Since $\left(a^{-1}\right)^{-1} = a$, any element of the form a^n can be written as $a^{-1-n} = \left(a^{-1}\right)^{-n}$. Clearly, since $n \in Z$, -n $\in$ Z. As a result, we can see that every element in G can be written as a power of a^{-1}. In other words, a^{-1} is a generator for G, or $G = \langle a^{-1} \rangle$.
   QED

3. Find all generators of Z_6 and Z_8.

   Solution: the generators of Z_6 are 1 and 5. We can see that 1 is a generator because

   $\langle 1 \rangle = \left\{1^n \mid n \in Z\right\} = Z_6 = G$. Here $1^0 = e, 1^1 = 1(1) = 1, 1^2 = 1(2) = 2, \ldots 1^5 = 1(5) = 5$, so

   $\langle 1 \rangle = \left\{0,1,2,3,4,5\right\} = Z_6 = G$, (Note: In such an additive group, $g^0 = g(0) = 0 = e$)
   Clearly since G is Cyclic, all other powers of g are just the same as one of those in z_6

   Similarly, we can show that 5 generates G because,
   $\langle 5 \rangle = \left\{5^n \mid n \in Z\right\} = \left\{5^0, 5^1, 5^2, 5^3, 5^4, 5^5\right\} = \left\{0, 5, 25, 15, 20, 125\right\} \equiv \left\{0, 5, 1, 3, 2, 4\right\} = Z_6 = G$.
   You should also verify that $\langle n \rangle \neq G\ \forall$ n $\in$ G, $n \neq 1, 5$!
   We can similarly find the generators in $G = Z_8 = \left(Z_{8,} +\right)$ to be 1,3,5,and 7.

You can see that this process is quite tedious. *However, we will prove later that all the generators of*
$G=(Z_n,+)=Z_n$ (Additive group understood since n not neccessarily prime!) *are those elements that are relatively prime to n.*

QED

4. Show in $G=(Z_n,+)$, for any $x\in G$, $|x|=|n-x|$.

Proof: Take x arbitrary from G. Then, $x+(n-x)=n\equiv 0$. So,

$x^{-1}=n-x\equiv -x \pmod{n}$

Recall that in any group, $|x|=|x^{-1}|$ (See Thm, in text/Proved in class notes). Thus,

$|x|=|n-x|$.

QED

5. Suppose G a group and $a\in G$. Show that if a has infinite order in G, then $a^m\neq a^n$ whenever $m\neq n$.

Proof: Assume $a^m=a^n$ and without loss of generality (WLOG) suppose $m<n$. Then $e=a^na^{-m}=a^{n-m}$, which contradicts the definition of infinite order. So, if a has infinite order in G, then $a^m\neq a^n$ whenever $m\neq n$.

QED

6. Let G be a group and let $a\in G$. Prove that $C(a)=C(a^{-1})$.

Proof: Suppose $x\in C(a)$. Then, $xa=ax\ \forall x\in G$. So, $a^{-1}(xa)=a^{-1}(ax)=x$. Thus, $(a^{-1}x)a=x$ and therefore $a^{-1}x=xa^{-1}\ \forall x\in G$. This shows that $x\in C(a^{-1})$. Thus, $C(a)\subseteq C(a^{-1})$. By symmetry, we can show $C(a^{-1})\subseteq C(a)$. Thus $C(a)=C(a^{-1})$.

QED

7. Prove that and abelian group with two elements of order 2 must have a subgroup of order 4.

Proof: Let G be such a group. Further suppose that for $a, b \in G$, $|a| = 2$ and $|b| = 2$.

The set $H = \{e, a, b, ab\}$ is *closed* (Note: e is guaranteed in G and a, b have the given properties by assumption. So, we can place them in H). H need only be *closed* to verify that H is a subgroup of G since H is finite (See the finite sub-group test).

QED

8. Prove that if G an Abelian Group with identity e, then $H = \{x \mid x \in G \text{ and } x^n = e\} \leq G$

(**Recall, in the special case when $n = 2$, we did not require abelian!**)

Proof: *We will prove this by the two-step subgroup test (more convenient than the one-Step !). Let $H = \{x \in G \mid x^n = e\}$. Since $e^1 = e,$* we have *$e \in H$ and H non-empty. Now, let $a, b \in H$. Then, $a^n = e$* and *$b^n = e$. So since G abelian, we have $(ab)^n = a^n b^n = ee = e.$ So, $ab \in H$ and H closed. To show inverses exist in H, again take $a \in H\cdot$ Since $a \in H,$* we have *$a^n = e\cdot$ Taking inverses of both sides, we obtain $(a^n)^{-1} = e^{-1} = e\cdot$ Since $(a^n)^{-1} = (a^{-1})^n$, we have $(a^{-1})^n = e\cdot$ It follows that $a^{-1} \in H$ and we have established inverses*. So, since $H \subseteq G$ is closed and obeys the inverse property, we have $H \leq G$ by the two-step subgroup test.

QED

9. Find the center of D_4, the dihedral group of order 8. Justify your answer.

Solution: By example 11 (p. 63) of the text, we have $Z(D_4) = \{R_0, R_{180}\}$ since n is even.

QED