Please write your proofs carefully and in complete English sentences. If you wish to use theorems from the text, make it clear which theorem you are using, by stating or describing it. Be careful to avoid using mathematical notation incorrectly. When in doubt, use English. Anything that the grader cannot understand may receive no credit.

Name: _____

1. (10 points) Let a be a group element of order n and suppose that m is a positive integer that is relatively prime to n. Show that there is an element y such that $y^m = a$.

   Hint: The phrase "relatively prime" should make you think immediately of a certain equation involving m and n.

Solution: Since m and n are relatively prime, there exist integers r and s such that $rm + sn = 1$. Then

$$a = a^1 = a^{rm+sn} = (a^r)^m (a^n)^s = (a^r)^m.$$

Thus, $a = y^m$, where $y = a^r$.

2. (a) (5 points) Give the definition of the *center*, $Z(G)$ of a group G.

Solution: The center of the group is the set of elements that commute with all elements of the group. That is,

$$Z(G) = \{g \in G \mid \text{for all } x \in G, \text{ gx=xg}\}.$$

(b) (5 points) Prove that $Z(G)$ is a subgroup of G.

Solution: Let g, h be elements of $Z(G)$. Let x be an element of G. Then

$$hx = xh.$$

If we multiply by h^{-1} on the right, we obtain

$$hxh^{-1} = x.$$

Then, multiplying by h^{-1} on the left yields

$$xh^{-1} = h^{-1}x.$$

Since x was an arbitrary element of G, this last equation shows that $h^{-1} \in Z(G)$. So, since h was an arbitrary element of $Z(G)$, we have proved that $Z(G)$ is closed under taking inverses. Next, since g and h belong to $Z(G)$, we have

$$(gh)x = g(hx) = g(xh) = (gx)h = (xg)h = x(gh).$$

Since x was an arbitrary element of G, this shows that $gh \in Z(G)$. As g and h were arbitrary elements of $Z(G)$, we have proved that $Z(G)$ is closed under products. We also see that the identity element e of G belongs to $Z(G)$. Therefore, $Z(G)$ is a subgroup of G.

3. True or false? If you think the statement is true, give a proof. If false, provide a concrete counterexample.

   (a) (3 points) The groups $U(n)$ are all cyclic.

   Solution: False. Consider $U(8) = \{1, 3, 5, 7\}$. The square of each element is equal to 1. In particular, no element can generate the whole group.

   (b) (4 points) If a, b are elements of a group such that $ab = ba$, then for all positive integers n, we have

   $$(ab)^n = a^n b^n.$$

   Solution:
   True. We give a proof by induction, starting at $n = 1$. Since $ab = ba$ by hypothesis, the statement is true for $n = 1$. Now assume that the statement holds for $n - 1$ and try to prove it for n. We have $(ab)^n = (ab)(ab)^{n-1}$. By the inductive hypothesis, we have $(ab)^{n-1} = a^{n-1}b^{n-1}$. Substituting, we have $(ab)^n = (ab)a^{n-1}b^{n-1}$. Now since $ba = ab$, we can switch the position of the b in the second place with each a in the a^{n-1} to get $(ab)^n = aa^{n-1}bb^{n-1} = a^n b^n$, as we wanted. This completes the induction step. Hence the statement holds for all positive integers n.

   (c) (3 points) If a group G has at least one element of infinite order, then all of its nonidentity elements have infinite order.

   Solution: False. In the multiplicative group of nonzero real numbers, 2 has infinite order, since there is no positive integer n such that $2^n = 1$. However, this group contains the nonidentity element -1 which has order 2.