Study guide

- Definitions: *order* of an element, order of a group (or subgroup), and the difference between the two.
- How do you prove that $o(x) = n$? What are the two things you must check?
- The exponent laws for groups (Theorem 4.1), and why they imply that $\langle g \rangle \leq G$.
- Know the formula: if $o(g) = n$, then $o(g^k) = n/(n,k)$ (Theorem 4.4(iii)), and some examples.
- Know the fact: if $o(g)$ is finite, then $g^k = e$ *if and only if* $o(g) \mid k$ (Theorem 4.4(ii)).
- Three number theory facts: the *division algorithm, Bézout's identity,* and *Euclid's lemma*.
- How do you use the division algorithm to show that $g^k = e \Rightarrow o(g) \mid k$? How do you use it to show that every subgroup of a cyclic group is cyclic?
- Know some examples of how Bézout's equation can be applied to group theory.

1. Suppose that G is an *abelian* group, and $x, y \in G$ are elements of finite order. Prove that if $(o(x), o(y)) = 1$, then $o(xy) = o(x)o(y)$.

2. Suppose that G is an abelian group with exactly 91 elements. Suppose that G has an element of order 7, and also an element of order 13. Prove that G is cyclic. (You may use the result of the exercise 1 in your argument even if you have not solved it yet).

   Comment: We will prove later that if p is a prime number dividing the number of elements in a finite group G, then G necessarily has an element of order p. So the exercise above implies that all abelian groups with 91 elements are cyclic.

3. The following statement is false, but it is true if it is revised slightly. Correct the statement and prove it: "If G is a cyclic group of order p, where p is prime, then every element of G is a generator of G."

4. Suppose that G is a finite group, and that the only subgroups of G are $\{e\}$ and G itself. Prove that the order of G is either 1 or a prime number.

5. Suppose that $G = \langle g \rangle$ is a cyclic group of order n. Prove that g^m is a generator of G if and only if $(m, n) = 1$.

6. Suppose that g is an element of a group G. Define the *centralizer* $Z(g)$ of g to be the set of all $x \in G$ that commute with g. In other words,

   $$Z(g) = \{x \in G : \; xg = gx\}.$$

   Prove that $Z(g)$ is a subgroup of G.

   Note The *centralizer* $Z(g)$ is different from the *center* $Z(G)$. It depends on *one element* $g \in G$, whereas the center depends on the whole group. They are related: the center is the intersection of all of the centralizers.

7. List all subgroups of the group $(\mathbb{Z}_{42}, \oplus)$.

8. Find all subgroups of Q_8 (the group of unit quaternions).

Note The group Q_8 is defined in Example 9 on page 47-8 of Saracino, which you should read before working on this problem. You may want to wait on this problem until after Tuesday, when we will discuss some strategies for classifying subgroups.