

Math 351:03 — Fall 1999

MW4 SEC-217

Prof. Bumby

Workshop 5, Review for exam.

In some of these problems, the division into parts is coarse, so that individual steps requiring proof are preceded with (●) as a reminder.

8*. If a group G has order pq where p and q are different primes, there are at most two possibilities for G up to isomorphism.

(a) If G is abelian, it must be cyclic. Let $g \in G$. By Lagrange's Theorem $g^{pq} = e$, so the least n such that $g^n = e$, denoted $o(g)$, is one of $1, p, q, pq$. If $o(g) = pq$, we have what we want. If $o(g) = 1$, $g = e$ and there are $pq - 1$ other elements of G to consider, so we choose a different g . If $o(g) = p$, then

$$H = \{ g^k : 0 \leq k < p \} \quad (*)$$

(●) has exactly p elements and forms a subgroup. Since G is abelian, (●) H is a normal subgroup. Consider G/H . (●) This has order q , so it is cyclic. If aH is not the identity (i.e., if $a \notin H$), then (●) $o(a)$ (the order of a as an element of G) is either q or pq . Again, if it is pq , we have what we want, so suppose $o(a) = q$. In this case $o(ag) = pq$. To see this, first (●) show that $o(ag)$ is divisible by q by showing that $(ag)^p H$ is not the identity of G/H ; then (●) show that $(ag)^q$, which is an element of H , is not e .

(b) If G is not abelian, (●) it cannot be cyclic, so (●) every element g other than the identity has $o(g) = p$ or $o(g) = q$. Suppose $o(g) = p$, and again form the subgroup H described by (*). Either H is a normal subgroup or not.

If H is normal, (●) every element a of G not in H has $o(a) = q$. Also $aga^{-1} \in H$, so (●) $aga^{-1} = g^b$ for some b . It then follows (by induction) that (●) $a^k ga^{-k} = g^{b^k}$. Since $a^q = e$, (●) $g^{b^q} = g$ and p divides $b^q - 1$. It is known that the $p - 1$ nonzero numbers modulo p form a cyclic group under multiplication, so the order of b in this group divides $p - 1$. This requires that q divide $p - 1$. In the original problem 8 we followed this argument with $p = 7$ and $q = 3$. We then took $b = 2$ and asked to (●) verify that this allows a multiplication to be defined on the set of all elements of the form $a^m g^n$. While this construction works in general, we confine attention to concrete examples such as this group of order 21 and various dihedral groups to allow all questions about the group to be settled by examining the elements.

If H is not normal, and $a \notin H$, $H \cap aHa^{-1} = e$. To prove this, first (●) show that any element of H other than the identity generates H , so that (●) $H = aHa^{-1}$ if the intersection is more than the identity. Then (●) $xHx^{-1} = H$ for all x of the form $a^m g^n$, but (●) every element of G can be written in this form. Then (●) extend this to show that two of the $a_i H a_i^{-1}$ with the a_i representing the q distinct cosets $a_i H$ can only intersect in the identity. This accounts for one identity and $q(p - 1)$ elements of order p , leaving only $q - 1$ other elements. These elements, together with the identity, (●) can only form a subgroup of order q . The previous analysis can then be applied. Again, these observations can be checked for the group of order 21 or a dihedral group of order $2n$ for $n = 2, 3, 4$, or 5 .

... continued on other side

11. The standard set of n elements is

$$\mathbf{n} = \{k \in \mathbb{Z} : 0 \leq k < n\},$$

so that $\mathbf{7} = \{0, 1, 2, 3, 4, 5, 6\}$. Then $m \leq n$ gives $\mathbf{m} \subseteq \mathbf{n}$. This can be used to consider S_m as a subgroup of S_n by identifying each S_n with $A(\mathbf{n})$. Given an element $f \in A(\mathbf{m})$, we define $\psi(f) \in A(\mathbf{n})$ by

$$(\psi(f))(k) = \begin{cases} f(k) & \text{if } k \leq m \\ k & \text{if } k > m \end{cases}$$

- (a) Show that ψ is a homomorphism.
- (b) Show that the kernel of ψ consists only of the identity.
- (c) In exercise 1.4.18, the set

$$U(T) = \{f \in A(S) : t \in T \implies f(t) \in T\}$$

was defined when $T \subseteq S$. If S is finite, extend the result of that exercise to show that $U(T)$ is a subgroup of $A(S)$.

- (d) Show that the image of ψ is a subgroup of $U(\mathbf{m})$.
- (e) Show that the image of ψ is a normal subgroup of $U(\mathbf{m})$, and find a description of the factor group.
- (f) If $m = 2$ and $n = 4$, how many elements are in each of these groups? (You may want to try this, and other small examples before working on a general result.)

12. For S taken to be the real numbers (in exercise 1.3.10, example 6 of section 2.1, and exercises referring to this example), the integers (in exercises 1.3.14 and 1.3.15), or the rational numbers (in exercise 1.3.21), functions of the form $f_{a,b}(s) = as + b$ with $a \in S$, $b \in S$ and $a \neq 0$ have been studied and, in some cases, shown to form a group. In example 7 of section 2.1, this is modified to allow b to be an arbitrary real number, while restricting a to be a nonzero rational number. After such frequent use, this seems to have been abandoned. Another extension that should be studied is to allow a and b to be complex numbers, again with $a \neq 0$.

- (a) For any of these examples, show that $f_{a,b}^n = f_{a^n, c_n(a)b}$, where

$$c_n(a) = \frac{a^n - 1}{a - 1}.$$

- (b) Use the formula in (a) to show that, with a and b complex and any n , there are solutions to $f_{a,b}^n = f_{1,0}$ other than $f_{1,0}$ itself. Note that, (•) in all of these cases, $f_{1,0}$ is the identity.
- (c) Illustrate this with $n = 3$. That is, show that, with complex coefficients, the conclusion of exercise 1.3.15 is more like 1.3.14 than the original statement with rational coefficients.