



## MATH 250A

PROFESSOR KENNETH A. RIBET

### First Midterm Exam

September 24, 2015

2:10–3:30 PM, Cory Hall Fan Room

Please write your NAME clearly:

Please put away all books, calculators, cell phones and other devices. You may consult a single two-sided sheet of notes. Please write carefully and clearly in *complete sentences*.

Problem	Your score	Possible points
1		6 points
2		6 points
3		6 points
4		6 points
5		6 points
Total:		30 points

These “solutions” are really quick guides to complete solutions. They were written by Ken Ribet on the morning of the exam and released on the course web site after the exam.

Note: If you want to suggest corrections to the solutions, please send me email and I’ll update this document.

If  $f: A \rightarrow A$  is an endomorphism of an abelian group, we write  $A_f$  for the kernel of  $f$  and  $A^f$  for the image of  $f$ .

**1a.** Let  $A$  be the group of non-zero complex numbers under multiplication, let  $f: A \rightarrow A$  be the map  $z \mapsto z/\bar{z}$ , and let  $g: A \rightarrow A$  be the map  $z \mapsto z\bar{z}$ . Show that  $f \circ g = g \circ f = 1$  and compute the index  $(A_f : A^g)$ .

The kernel of  $f$  consists of the non-zero complex numbers that are equal to their complex conjugates. These complex numbers are the non-zero real numbers. The image of  $g$  consists

of non-zero real numbers of the form  $z\bar{z}$ , where  $z$  is complex. Thus the image consists of positive real numbers. The sought-after index is thus 2.

**b.** If  $z$  is a complex number different from 1 such that  $z\bar{z} = 1$ , show that

$$\frac{i - zi}{-i + \bar{z}i} = z.$$

Use this formula to compute the index  $(A_g : A^f)$ .

The index is 1; we are proving that complex numbers of norm 1 (i.e., those in the kernel of  $g$ ) are all of the form  $w/\bar{w}$ . (Numbers of this form obviously have norm 1.) The particular complex number 1 is certainly of the form  $w/\bar{w}$ : we take  $w = 1$ . Suppose that  $z$  is different from 1 and satisfies  $z\bar{z} = 1$ . Then the displayed formula shows that  $z = w/\bar{w}$ , where  $w = i - zi$ . Thus the displayed formula implies what we want. Checking the displayed formula is just a matter of a quick computation. (It's probably a good idea to cross multiply to clear the denominator.)

**2.** Let  $G$  be a group of order  $2^2 \cdot 5 \cdot 17$ . Show that  $G$  has normal subgroups  $H$  and  $K$  of order 5 and 17, respectively. Show also that the set  $HK$  is a normal subgroup of  $G$ .

The groups  $H$  and  $K$  are, respectively, the unique Sylow subgroups of  $G$  of order 5 and 17. The subgroups are unique because the numbers of Sylows, usually denoted  $n_5$  and  $n_{17}$ , satisfy divisibility and congruence properties that force them to be 1. Because  $H$  normalizes  $K$  (or vice versa), the set  $HK$  is a subgroup of  $G$ . Its order is 85, by the way, because  $H$  and  $K$  have trivial intersection. Also the subgroup is normal because  $H$  and  $K$  are individually normal: If you conjugate a product  $hk$ , you get the product of the conjugates of  $h$  and  $k$ . But the conjugate of  $h$  is in  $H$  and the conjugate of  $k$  is in  $K$ .

**3.** Suppose that a group  $G$  acts on a set  $X$  and that both  $G$  and  $X$  are finite. For each  $g \in G$ , let

$$\text{Fix}_g(X) = \{x \in X \mid gx = x\}.$$

Show that the average value of  $\#\text{Fix}_g(X)$ , namely

$$\frac{1}{\#G} \sum_{g \in G} \#\text{Fix}_g(X),$$

is the number of orbits for the action of  $G$  on  $X$ .

This was a homework problem from the first week; see problem 19 on page 77. To do it, you can carve up  $X$  into its various orbits and consider separately the action of  $G$  on each orbit. An orbit is a  $G$ -set of the form  $G/H$ , where  $H$  is a subgroup of  $G$ ; we need consider only this case. The aim in this situation is to prove that the "average value" of the problem is 1 because there's only one orbit.

The set  $\text{Fix}_g(X)$  is the number of  $x$  such that  $gx = x$ . The sum  $\sum_{g \in G} \#\text{Fix}_g(X)$  counts the number of pairs  $(g, x)$  with  $gx = x$ . The point of the problem is to count these pairs by fixing  $x$  and seeing how many  $g \in G$  satisfy  $gx = x$ . The set of  $g$  with  $gx = x$  is the stabilizer

of  $x$ , so the sum  $\sum_{g \in G} \# \text{Fix}_g(X)$  is the sum of the orders of the stabilizers of the various points of  $X = G/H$ . The points of  $G/H$  are the cosets  $tH$  with  $t \in G$ , and the stabilizer of  $tH$  is  $tHt^{-1}$ , which has order  $\#(H)$ . Since the number of points of  $G/H$  is the index  $(G : H)$ , the sum  $\sum_{g \in G} \# \text{Fix}_g(X)$  is  $(G : H) \cdot \#(H) = \#(G)$ . When we divide by the denominator  $\#(G)$ , we get 1, which is the answer that we were hoping for.

**4.** Let  $G$  be the group of invertible  $n \times n$  matrices with coefficients in the field  $\mathbf{Z}/p\mathbf{Z}$  of integers mod  $p$ . Let  $P$  be a subgroup of  $G$  of  $p$ -power order. Show that there is a conjugate of  $P$  in  $G$  that consists entirely of upper-triangular matrices.

Let  $Q$  be the group of upper-triangular matrices with 1s on the diagonal. As we saw in our proof of the Sylow theorems, the group  $Q$  is a  $p$ -Sylow subgroup of  $G$ . Since  $P$  is a  $p$ -group, we know from the standard Sylow theorems that  $P$  is contained in a conjugate of  $Q$ . Symbolically,  $P \subseteq gQg^{-1}$  for some  $g \in G$ . Conjugating by  $g^{-1}$  then gives  $g^{-1}Pg \subseteq Q$ , which gives us the right to say “QED.”

Another way to prove the desired result is to notice that conjugation in  $G$  amounts to choosing a new basis of  $(\mathbf{Z}/p\mathbf{Z})^n$ . You can build up a suitable basis using induction. To begin the construction, you want to find the first element of the basis; this would be a non-zero vector in  $(\mathbf{Z}/p\mathbf{Z})^n$  this is fixed by (each element of)  $P$ . Such a vector exists because of the lemma that the number of  $P$ -fixed vectors is congruent mod  $p$  to the number of all vectors; thus the number of  $P$ -fixed vectors is divisible by  $p$ . Since 0 is obviously a  $P$ -fixed vector, there must be non-zero vectors that are fixed by  $P$  as well.

**5.** Prove that a finite abelian group is cyclic if it has this property: for each  $n \geq 1$ , the group contains at most  $n$  elements of order dividing  $n$ .

We can use the sledgehammer of the lecture on September 17 to write the group as a direct sum  $\mathbf{Z}/a_1\mathbf{Z} \oplus \mathbf{Z}/a_2\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/a_t\mathbf{Z}$ , where the  $a_i$  are integers bigger than 1 and where  $a_1|a_2$ ,  $a_2|a_3$ , etc. The number of elements of this direct sum of order dividing  $a_1$  is  $a_1^t$ . Since this number is supposed to be at most  $a_1$ , we have  $t = 1$ , implying that the group is the cyclic group  $\mathbf{Z}/a_1\mathbf{Z}$ .