Mathematics 113 Professor K. A. Ribet

First Midterm Exam September 26, 2013

Morning Edition

> 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.* Your explanations are your only representative when your work is being graded.

The problems have equal weight.

1. If H is a subgroup of $\mathbf{Z}$ (the group of integers under addition), prove that there is an integer $n \geq 0$ such that H is the set of integer multiples of n.

We did this in class. There are two possibilities. The first is that $H = \{0\}$. The second is that H isn't $\{0\}$. In the first case, take $n = 0$. In the second, show that H contains positive integers and let n be the smallest positive integer in H. The equality $H = n\mathbf{Z}$ follows by Euclidean division.

2. Let n and m be integers ≥ 3. Suppose that there is a surjective ("onto") homomorphism $D_{2n} \to D_{2m}$. Show that n is a multiple of m.

A sophisticated way to do this is to invoke the general fact that when there's a surjective homomorphism between finite groups, the order of the source group divides the order of the target. This fact follows from the natural isomorphism between the image of a homomorphism and the quotient group gotten by dividing the source group by the kernel of the homomorphism. To complete the proof using this kind of argument, you need to recall the formula that the order of a quotient group G/K is the order of G divided by the order of K; this formula becomes visible as one proves Lagrange's theorem.

If I had intended this kind of argument, I wouldn't have framed the problem about specific groups (dihedral groups). Here's something a bit more concrete. Suppose that f is a homomorphism as in the statement of the problem. Since f is surjective, there is an $x \in D_{2n}$ that maps to the element r of D_{2m}. Let t be the order of x. Then $x^t = 1$, and so $f(x)^t = 1$. Since $r = f(x)$ has order m, t is a multiple of m. Now think about the orders of elements of D_{2n}. There's 1, which has order 1. There are the elements sr^i, which have order 2. And then there are the elements r^j, whose orders divide n. Since t is a multiple of m, which is at least 3, t must be at least 3 and therefore x is an r^j and thus has order dividing n. Then m divides t, which in turn divides n. Thus m divides n.

3. [The first paragraph was just background.] If n is a positive integer, recall that $\mathbf{Z}/n\mathbf{Z}$ is the group of mod n integers under addition and that $(\mathbf{Z}/n\mathbf{Z})^*$ is the group of invertible mod n integers under multiplication. Recall further that a mod n is invertible if and only if a and n are relatively prime (i.e., have gcd = 1). The group $G = (\mathbf{Z}/n\mathbf{Z})^*$ operates on the set $A = \mathbf{Z}/n\mathbf{Z}$ by multiplication: for $g \in G$ and $a \in A$, $g \cdot a$ is the product of g and a mod n.

[This is the question:] For $a \in \mathbf{Z}/n\mathbf{Z}$, establish a formula (in terms of a and n) for the order of the stabilizer G_a.

The stabilizer in question is the set of $x \in (\mathbf{Z}/n\mathbf{Z})^*$ for which $(x-1)a = 0 \in \mathbf{Z}/n\mathbf{Z}$. If a is invertible, for example, then we have $x - 1 = 0$; thus the stabilizer has one element. If $a = 0$, which is the example at the other end of the spectrum, then G_a is all of G; the order of this group is known as $\varphi(n)$. (That's just a definition, but we can say that $\varphi(n)$ is a quantity that's written "in terms of n." Also, there are well known formulas for $\varphi(n)$ in terms of the prime factorization of n.)

To discuss the general case, note that the requirement that x stabilizes a means that x has to be congruent to 1 mod n/t; this is what it will take to make product $(x-1)a$ be divisible by n. To make the notation more pleasant, let's introduce $m := n/t$. Then of course $n = t \cdot m$. The stabilizer of a is the kernel of the map $(\mathbf{Z}/n\mathbf{Z})^* \to (\mathbf{Z}/m\mathbf{Z})^*$ that takes $x \pmod{n}$ to $x \pmod{m}$. It's fairly obvious by the Chinese Remainder Theorem that this map is surjective (onto). I'll consider this fact as known, but you can ask me for more info if you wish. The main point for me is that if K is the kernel of a surjective map $G \to G'$ between finite groups, then the order of K is the ratio of the orders of the two groups: the order of G divided by the order of G'. In this case, the order of the kernel (which is the order of the original stabilizer) is $\varphi(n)/\varphi(m)$.

I must say that I need to apologize here for the fact that I seem to be using information from Tuesday's lecture, which was not supposed to be in the scope of the exam. I intended originally to have n be a specific integer, namely 3^5. That would have made the problem more concrete and easy to deal with. I promise to be generous with partial credit.

4. Find the 20th power of the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 4 & 8 & 1 & 10 & 5 & 6 & 9 & 3 & 2 \end{pmatrix}$.

If I remember correctly, this permutation is the disjoint product of a 7-cycle and a 3-cycle. Accordingly, it has order 21. Its 20th power is then its inverse, which takes 1 to 4, 2 to 10, etc.

5. Let Ω be the set of positive integers. For each positive integer n, describe an element of order n in the symmetric group S_Ω.

We can take the n-cycle $(1\,2\,\cdots n)$, which moves the first n integers and leaves the other positive integers untouched.