Mathematics 113 — Professor K. A. Ribet

First Midterm Exam — September 26, 2013

Afternoon 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. Suppose that G is a finite group and that $g \in G$ has order n (where n is a positive integer). Let i be an integer. Find a formula for the order of g^i and prove that your formula is correct.

The order is $n/gcd(n, i)$. I won't prove the formula here; see Prop. 5, p. 57 in the textbook.

2. Suppose that H is a finite group in which each non-identity element has order 2. Prove that H is abelian.

The hypothesis means that every element of H is its own inverse: for $x \in H$, $x \cdot x = 1$. If $x, y \in H$,

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx.$$

To say that $xy = yx$ for every x and y is to say that the group is abelian.

3. Let x be an element of the dihedral group D_{2n} $(n \geq 3)$. Describe explicitly the set of conjugates of x (i.e., the set of elements of the form gxg^{-1}). Treat separately the cases where x is a power of r and where x is not a power of r.

The element r is sent to r^{-1} when it's conjugated by s and is unchanged when it's conjugated by r. If you conjugate by a product gg', you just conjugate by g' and then conjugate the result by g. Because all elements of the group "can be expressed in terms" of r and s, the only conjugates of r are r and r^{-i}. Since conjugation is a homomorphism, the only conjugates of a power r^i of r are r^i and r^{-1}. Note, however, that r^i can occasionally be equal to r^{-i}: this happens when $2i \equiv 0$ mod n. If n is odd, this congruence is equivalent to having i be 0 mod n, but if n is even, i can also be $n/2$ mod n. Accordingly, a power of r has one or two distinct conjugates. The case of one conjugate occurs exactly when $r^i = r^0$ is the identity and (if n is even) when $r^i = r^{n/2}$.

How about the conjugates of sr^i? If you conjugate sr^i by r^j, you should get (= I got) sr^{i-2j}. If n is odd, the exponents $i - 2j$ represent all numbers mod n as i stays fixed and j varies mod n. If n is even, the number of exponents $i - 2j$ mod n is $n/2$: you get all the numbers mod n that have the same parity as i. Thus we get either n or $n/2$ conjugates by conjugating sr^i by r^j.

But we can also conjugate sr^i by elements of the form sr^j. Conjugating sr^i by sr^j is the same as conjugating by r^j and then conjugating the result by s. If you conjugate sr^{i-2j} by s, you get sr^{2j-i}. As j varies, you again get either all possible sr^k or only half of them: the ones for which k has the same parity as i. In other words, you get the same elements of G by conjugating sr^i by the r^j as by conjugating by the sr^j. All told, sr^i has either n or $n/2$ conjugates, depending on whether n is odd or even.

4. Let σ be the 20-cycle $(1 \quad 2 \quad 3 \quad 4 \quad \cdots \quad 17 \quad 18 \quad 19 \quad 20)$. What are the different cycle types that occur as we consider the various powers of σ? For which integers i is σ^i a 20-cycle?

The order of σ^i is a divisor of 20; the divisor in question was calculated in problem 1. Say the order is m. Then σ^i is a product of various m-cycles. The number of cycles in the product is $20/m$. The case $m = 20$ occurs precisely when i and 20 are relatively prime.

5. Let p be a prime number. Find the number of invertible matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $a, b, c, d \in \mathbf{Z}/p\mathbf{Z}$. For $t \in (\mathbf{Z}/p\mathbf{Z})^*$, show that the number of such matrices with determinant t is equal to the number of such matrices with determinant 1. What is the latter number?

The number of 2×2 invertible matrices over $\mathbf{Z}/p\mathbf{Z}$ was calculated in a homework problem; the answer was $(p^2 - 1)(p^2 - p)$. I hope that you recall this formula and explain how it was derived.

The set of matrices with determinant t is in 1-1 correspondence with the set of matrices with determinant 1. You get back and forth between the two sets by multiplying by the matrix $\begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix}$ or its inverse. Hence the number of invertible matrices with determinant t is independent of t as t runs over the non-zero numbers mod p. There are $p - 1$ such numbers, so the number of matrices with given non-zero determinant is $\dfrac{(p^2 - 1)(p^2 - p)}{p - 1}$. This number is, in particular, the number of matrices with determinant 1.