Math H113 Professor K. A. Ribet
Final Exam May 16, 2003

Please put away all books, calculators, electronic games, cell phones, pagers, .mp3 players, PDAs, and other electronic devices. Please write your name on each sheet of paper that you turn in; don't trust staples to keep your papers together. Explain your answers in full English sentences as is customary and appropriate. Your paper is your ambassador when it is graded.

These solutions were written quickly by Ken Ribet. Sorry if they're a little terse. They're perhaps best described as sketches of solutions.

1. Let H be a subgroup of a finite group G. For each g in G, consider the subset $S_g := H(gHg^{-1})$ of G; this is the subset HK where $K = gHg^{-1}$. Show that H is normal in G if and only if all the sets S_g have the same size.

In general, the order of HK is $\dfrac{|H||K|}{|H \cap K|}$. To say that the S_g have the same size is to say that all the intersections $H \cap gHg^{-1}$ have the same size. When $g = 1$, the intersection is H; in general, the intersection is contained in H. The intersections have the same size exactly when gHg^{-1} contains H for all g. This comes down to the statement that H is normal in G.

2. Let p and q be distinct primes. Show that every group of order p^2q has a normal Sylow subgroup. [You can assume that p^2q is different from 12, since we studied groups of order 12 in class.]

Let P and Q be p- and q-Sylow subgroups. The number of conjugates of P divides q and is 1 mod p. If it's 1, where done. Suppose otherwise; then the number of conjugates is q and we have $q \equiv 1 \bmod p$. The number of conjugates of Q divides p^2 and is 1 mod q. It can't be p because p is smaller than q. If it's not 1, then it's p^2 and we have $p^2 \equiv 1 \bmod q$. This means that q divides $p^2 - 1 = (p+1)(p-1)$. Clearly, q does not divide $p - 1$, as was said already: this is because p is smaller than q. Since q is a prime, it follows that q divides $p + 1$. We must then have $q = p + 1$ because p is smaller than q. This leads to the conclusion that $p = 2$ and $q = 3$; 2 and 3 are the only two consecutive prime numbers. The case $p = 2$, $q = 3$ requires a further argument, but we gave it in class, as I said in the statement of the problem.

3. Let G be a finite abelian group. Suppose that the intersection of all non-identity subgroups of G is a non-identity subgroup of G. Prove that G is isomorphic to $\mathbf{Z}/p^n\mathbf{Z}$ for some prime p and some positive integer n.

If x and y are non-identity elements of G, then their orders cannot be relatively prime; if the orders were relatively prime, then the cyclic groups $\langle x \rangle$ and $\langle y \rangle$ already would have trivial intersection, contrary to the assumption. It's tempting here to invoke Cauchy's *theorem to the effect that G has an element of order p for each prime p dividing $|G|$. This theorem clearly implies that only one prime can divide the order of G; say this prime is p. The idea now is that G should be the cyclic subgroup generated by x if the order of x is the largest order of elements of G. This statement clearly follows from the following one, which we will prove by induction on n: Suppose that x and y are elements of G of order p^n and p^i, respectively. Assume that we have $i \leq n$. Then y is a power of x. This statement is true when $n = 1$ because, by hypothesis, G contains at most one subgroup of order p. Working by induction (and writing G additively now!), we can write py as a multiple of px, say $py = t \cdot px$. Then $y - tx$ has order dividing p, so it's a multiple of x. We get, finally, that y is a multiple of x, which is what we needed.*

4. Let A be a non-empty set and let G be a subgroup of the group S_A of permutations of A. For $a \in A$, let $G_a = \{\, g \in G \mid ga = a \,\}$. Show that $G_{ga} = gG_ag^{-1}$ for $g \in G$, $a \in A$. If G acts transitively on A, show that $\displaystyle\bigcap_{g\in G} gG_ag^{-1} = \{1\}$ for each $a \in A$.

Further, if G is an abelian subgroup of S_A that acts transitively on A, show that $G_a = \{1\}$ for all $a \in A$. Prove that $|G| = |A|$ in this case.

We have an action of a group G on a set A. The group G_a is the stabilizer of a, a group that we studied a lot. We proved the equality $G_{ga} = gG_ag^{-1}$ in class, probably more than once. I hope that you all recalled the proof in your answer. The point of this is that, for each a, the intersection $\displaystyle\bigcap_{g\in G} gG_ag^{-1}$ may be viewed as the set of elements of G that fix all ga. When the action of G on A is transitive, this is the set of elements of G that fix everything, i.e., that act trivially on A. Because G here is a subgroup of S_A, an element of G that fixes all of A is the identity element. In the case where G is abelian, gG_ag^{-1} is the same thing as G_a, so the intersection is just G_a. This implies that $G_a = \{1\}$, as required; in words, we can say that non-identity elements of G fix no elements of A. Take $a \in A$, which is possible because A is non-empty. The map $G \to A$ given by $g \mapsto ga$ is then injective because of what we said about non-identity elements not fixing anything. It's surjective because the action of G on A was supposed to be transitive. So it's a bijection and we get the equality $|G| = |A|$.

5. Consider the evaluation homomorphism $\varphi : \mathbf{R}[x] \to \mathbf{C}$ that sends each polynomial $f(x)$ to the complex number $f(2+3i)$. Find a generator for the kernel of φ. *If f vanishes on $2+3i$, it vanishes on $2-3i$ as well. Hence, as a complex polynomial, it is divisible both by $x-(2+3i)$ and $x-(2-3i)$. By unique factorization, it will be divisible by $p(x) := (x-(2+3i))((x-(2-3i)) = x^2-4x+13$ in $\mathbf{C}[x]$. This suggests that the kernel of φ is $(p(x))$, the ideal generated by $p(x)$ in $\mathbf{R}[x]$. To see this, we let $\alpha = 2+3i$ and note that α is a root of p but not of any non-zero polynomial of degree ≤ 1 over $\mathbf{R}$. If f is a polynomial with real coefficients, we divide f by p and get an equation $f(x) = q(x)p(x) + r(x)$ with r of degree less than 2. Because $p(\alpha) = 0$, $f(\alpha) = 0$ if and only if $r(\alpha) = 0$, which happens if and only if $r(x) = 0$. Thus the kernel of φ consists of the multiples of p.*

6. Let n be a positive integer, and let p be a prime number that divides $2^n + 1$. If m is an odd positive integer, show that p does not divide $2^m - 1$. *Since p divides $2^n + 1$, p is not 2, so we can consider 2 mod p as an element of $(\mathbf{Z}/p\mathbf{Z})^*$. In this group $2^n = -1$, an element of order 2. Since the order of any power of 2 divides the order of 2, 2 has even order in $(\mathbf{Z}/p\mathbf{Z})^*$. This means that 2^m can never be 1 in $(\mathbf{Z}/p\mathbf{Z})^*$ if m is an odd number. That's exactly what was to be proved.*

7. Is an irreducible element of an integral domain necessarily prime? (Give a proof or a counter-example.)

We know that the answer is "no" because we've seen examples in class. The whole point of our discussions of irreducibility was to prove in certain circumstances (e.g., for a PID) that irreducible elements are prime.

If R is a commutative ring with 1, it is true that the intersection of two maximal ideals of R is a prime ideal? (Proof or counter-example.)

This is kind of silly. In $\mathbf{Z}$, the intersection of the maximal ideals (2) and (3) is the ideal (6), which is not prime.

If R is a commutative ring with 1, is it necessarily true that $1 - x$ is a unit if $x^9 = 0$? (Proof or counterexample.)

It's true. The element $1 + x + \cdots + x^7 + x^8$ is the inverse of $1 - x$.

8. Let $n \geq 3$ be an odd integer. Show that the dihedral group D_{2n} of order $2n$ has exactly $(n + 3)/2$ conjugacy classes.

Find a finite group G and a subgroup H of G so that H has more conjugacy classes than G.

Let $D = D_{2n}$. This group has a cyclic subgroup C of order n. The elements of D outside of C are of order 2 and they're all conjugate to each other. The identity element of D makes up its own conjugacy classes. So far, we've seen two conjugacy classes. The $n - 1$ non-identity elements of C form $(n-1)/2$ conjugacy classes in D: conjugation by elements of D outside of C induces the inversion map $x \mapsto x^{-1}$ on C, so that each $x \in C$ is conjugate only to itself and to its inverse. The number of conjugacy classes is $2 + (n - 1)/2$, which is the same number as $(n + 3)/2$. Now C is abelian, so it has n conjugacy classes. Thus C has more conjugacy classes than D as soon as n is bigger than $(n + 3)/2$. This happens, e.g., when $n = 7$.