Math 250A, Fall 2004
Final Exam—December 20, 2004

Please put away all books, calculators, electronic games, BlackBerries, cell phones, pagers, .mp3 players, PDAs, and other electronic devices. You may refer to a single 2-sided sheet of notes. Explain your answers in full English sentences as is customary and appropriate. Your paper is your ambassador when it is graded.

1. *Show that every group of order 56 has a non-trivial proper normal subgroup.*

Let G be a group of order 56. The number of 7-Sylow subgroups is 1 mod 7, and it's a divisor of 8. If there is one 7-Sylow, it's notmal and we're done. Assume that there are 8. Then there are $6 \cdot 8 = 48$ elements of order 7 in G, so that there are only 8 elements that are not of order 7. It is clear now that there is a unique 2-Sylow subgroup: a 2-Sylow subgroup has order 8, and it must be precisely the set of elements of G that are not of order 7.

2. *Suppose that G is a finite group. Let N be a normal subgroup of G and let H be a subgroup of G. If the order of H is prime to the index $(G : N)$, show that H is contained in N.*

Consider the natural map $H \to G/N$ gotten by compositing the inclusion of H in G with the projection $G \to G/N$. The image of this map has order dividing the order of H and also has order dividing the order of G/N (which is the index of N in G). Hence the image is trivial, which means that H is contained in N.

If the order of N is prime to the index $(G : H)$, show that N is contained in H.

The set HN is a subgroup of G because G is normal. Note that $(HN : H)$ is a divisor of $(G : H)$, so it's prime to the order of N. Now $\#(HN) = \#(H)\#(N)/\#(H \cap N)$, so that $(NH : H) = \#(NH)/\#(H) = \#(N)/\#(H \cap N)$. This divisor of $\#(N)$ is supposed to be prime to $\#(N)$, so it must be 1. This means that $H \cap N = N$, so that N is contained in H.

3. *Let n be an integer greater than 1, and let p be an odd prime number. Set $f(X) = X^n + X + p$. Show that all complex roots of f have absolute value bigger than 1.*

If α is a complex number of absolute value ≤ 1, then $|\alpha^n| \leq 1$, so we get $|\alpha + \alpha^n| \leq 2 < p$; thus we cannot have $\alpha^n + \alpha + p = 0$.

Prove that $f(X)$ is irreducible over $\mathbf{Q}$.

By Gauss's lemma, it is enough to prove that $f(X)$ cannot be factored over $\mathbf{Z}$. Assume that there is a non-trivial factorization $f(X) = g(X)h(X)$ with $g, h \in \mathbf{Z}[X]$. The product of the top coefficients of g and h is 1; after changing signs, we can and will assume that g and h are monic. The constant coefficients of g and h multiply to the prime number p. After permuting g and h, we can and will assume that $g(0) = \pm 1$. The product of the roots of g is then ± 1; because g is non-constant, g does have complex roots. Since the roots of g lie among the roots of f, we have a contradiction: a product of numbers of absolute value bigger than 1 cannot be equal to 1.

4. *Suppose that E and F are finite Galois extensions of a field k, with E and F both contained in a common extension L of k. Which of the following extensions of k are necessarily Galois extensions of k (sketch a proof or provide a counterexample): The compositum EF of E and F.*

Sure, this extension is well known to be Galois. If E and F are the splitting fields of families of separable polynomials, then EF is the splitting field of the big family gotten by throwing together the polynomials that give E and F.

The intersection $E \cap F$.

The intersection is again Galois over k. One way to see this is to say that $E \cap F$ is a subfield of E and is therefore separable over k. The issue is whether or not it's normal. Any $\sigma : E \cap F \to \overline{k}$ that's the identity on k can be extended to a map $E \to \overline{k}$ and therefore takes values in E (because E is normal over k). Symmetrically, it takes values in F. Therefore, the image lies in $E \cap F$. An alternate argument is to exploit the corollary that you proved for the last HW assignment. If the subgroups of $\mathrm{Gal}(L/k)$ that correspond to E and F are H and H', then the subgroup corresponding to the intersection is the group generated by H and H'. If H and H' are both normal subgroups of $\mathrm{Gal}(L/k)$, so is the group that they generate together.

5. *The product of two objects A and B of a category $\mathcal{C}$ is an object P of $\mathcal{C}$ together with morphisms $f \in \mathrm{Mor}(P, A)$, $g \in \mathrm{Mor}(P, B)$. The definition of "product" requires that triple (P, f, g) satisfy a certain condition. What condition?*

The condition is usually parphrased as follows: to map an object X to A and to B is to map it to P. More precisely, the map

$$\mathrm{Mor}(X, P) \to Mor(X, A) \times Mor(X, B), \qquad h \mapsto (f \circ h, g \circ h)$$

is a bijection for each X.

Suppose now that $\mathcal{C}$ is the category whose objects are the positive integers. Define morphisms such that, for integers $n, m \geq 1$, $\mathrm{Mor}(n, m)$ is the set of real $m \times n$ matrices (m rows and n columns) and such that, for integers $n, m, l \geq 1$, the composition law $\mathrm{Mor}(n, m) \times \mathrm{Mor}(l, n) \to \mathrm{Mor}(l, m)$ is ordinary matrix multiplication. What is the product of n and m in $\mathcal{C}$?

See `http://math.berkeley.edu/~ribet/250/Fall01/mt1ans.pdf` . The short answer is that the product is $n + m$.

6. *Suppose that K/k is a finite Galois extension and that $\alpha_1, \ldots, \alpha_n$ are distinct elements of K. Assume further that the polynomial $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ has coefficients in k. Show that $f(x)$ is irreducible over k if and only if the natural operation of $\mathrm{Gal}(K/k)$ on $\{ \alpha_1, \ldots, \alpha_n \}$ (by conjugation) is transitive.*

If f is reducible–say $f = gh$ in $k[x]$, then the action of $\mathrm{Gal}(K/k)$ on the roots of f sends roots of g to roots of g and roots of h to roots of h. Thus the action is not transitive: you can't find an element of $\mathrm{Gal}(K/k)$ that sends an aribtrary α_i to an arbitrary α_j. Suppose that f is irreducible, and take two roots α_i and α_j of f. As we know, there are isomorphisms $k[x]/(f(x)) \xrightarrow{\sim} k(\alpha_i)$ and $k[x]/(f(x)) \xrightarrow{\sim} k(\alpha_j)$ that map x to α_i and α_j, respectively. Taking the composite of one map and the inverse of the other, we obtain $\sigma : k(\alpha_i) \to k(\alpha_j)$ that sends α_i to α_j and is the identity on k. View σ as an embedding $k(\alpha_i) \to K$ and extend it to an automorphism of K. The resulting element of $\mathrm{Gal}(K/k)$ sends α_i to α_j.