Math 114 Professor K. A. Ribet
Final Exam May 21, 2004

This exam was a 3-hour exam. It began at 3:40PM. There were 6 problems, with all but the second problem counting for 5 points. The second (multi-part) problem was worth 20 points. Thus the maximum possible score was 45.

Please put away all books, calculators, electronic games, cell phones, pagers, .mp3 players, PDAs, and other electronic devices. You may refer to a single 2-sided sheet of notes. 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. If you invoke a theorem that we proved in class, state the theorem clearly and explain carefully how you are applying it. You may use the equation $999 = 27 \cdot 37$ *without justifying it. Your paper is your ambassador when it is graded.*

This solution sheet is a living document. (I wrote it up quickly.) If you find typos or mistakes, or if you want more clarification, send me e-mail.

1. *Let* $f(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0$ *be a monic polynomial with integer coefficients. Suppose that* $f(t)$ *is the product* $g(t)h(t)$ *where* g *and* h *are monic polynomials with rational coefficients. Show that* g *and* h *have integral coefficients.*

Suppose that $D \geq 1$ and $D' \geq 1$ are denominators for g and h, respectively; this means that $G = Dg$ and $H = D'h$ are polynomials with integral coefficients. Then $G(t)H(t) = DD'f(t)$ is divisible by DD' in the obvious sense that all of its coefficients are divisible by DD'. Let d be the gcd of the coefficients of $G(t)$ and let d' be the gcd of the coefficients of $H(t)$. Then of course d divides D because the top coefficient of G is D (since g was monic); similarly, d' divides D'. However, the principle of Gauss's Lemma (p. 39 of our book) is that DD' divides dd'. ("We can cancel out prime factors..., one by one, without going outside $\mathbf{Z}[t]$.") In words: if a product of two polynomials is divisible by DD', then we can explain this divisibility by looking at the two factors. Comparing our divisibilities, we see that $d = D$ and $d' = D'$. Hence G is divisible by D, which means that $G(t)/D = g(t)$ is an integral polynomial. Similarly, $h(t)$ is integral.

2. *In each of the following five situations, find the Galois group* $G = \mathrm{Gal}(\Sigma/K)$*, where* Σ *is the splitting field of* $f(t)$ *over* K*. If you are able to calculate only* $[\Sigma : K]$*, but not* G*, please provide this degree. The symbol "p" denotes a prime number.*

a. $K = \mathbf{Q}$, $f(t) = t^{16} + 1$.

A root of this polynomial is a number whose 16th power is -1. Numbers with this property are the 32nd roots of 1. When we adjoin a single root of f to $\mathbf{Q}$, we make the field of 32nd roots of unity, whose Galois group is a priori a subgroup of $(\mathbf{Z}/32\mathbf{Z})^*$, which is a group of order 16. We proved in class, toward the end of the semester, that the Galois group

of the field of nth roots of 1 is the full group $(\mathbf{Z}/n\mathbf{Z})^*$ whenever n is a positive integer (prime or not). Thus $\Sigma : \mathbf{Q}$ has degree 16 in this case. You can see this alternatively by considering $f(t+1)$, which is an Eisenstein polynomial at 2: its constant coefficient is 2, and it looks like t^{16} mod 2 because squaring is additive mod 2. I glanced at exam papers as they were turned in and saw that some students had asserted that $(\mathbf{Z}/32\mathbf{Z})^*$ is a cyclic group of order 16. This is not so, as we can see from the fact that 17 and 31 are two non-identity elements of $(\mathbf{Z}/32\mathbf{Z})^*$ whose squares are 1. In a cyclic group, there can be at most one element of order 2.

b. $K = \mathbf{Q}(e^{2\pi i/5})$, $f(t) = t^5 - 100$.

The splitting field of f over K is the same as the splitting field of f over $\mathbf{Q}$, since we have the fifth roots of 1 once we have all fifth roots of 100. The polynomial f is irreducible over $\mathbf{Q}$. Indeed, the polynomial $t^5 - 10$ is irreducible by Eisenstein's criterion (for the prime 5 or the prime 2). Thus if α is a root of $t^5 - 10$, $\mathbf{Q}(\alpha)$ has degree 5 over $\mathbf{Q}$. The number α^2 is a root of f, and it is clear that $[\mathbf{Q}(\alpha) : \mathbf{Q}(\alpha^2)] \leq 2$ because α is the square root of a number in $\mathbf{Q}(\alpha^2)$. By the tower law, we see that $[\mathbf{Q}(\alpha^2) : \mathbf{Q}] = 5$, so that f is irreducible as was claimed. It follows that $[\Sigma : \mathbf{Q}]$ is divisible by 5. Since $[K : \mathbf{Q}]$ is prime to 5 (it's 4, in fact), 5 divides $[\Sigma : K]$. However, it is clear that $\Sigma = K(\beta)$ whenever β is a root of f; this is because the various roots of f will be products $\beta\zeta$ for numbers ζ that are in K already. Hence $\Sigma : K$ has degree less than or equal to the degree of f, which is 5. Putting all of this together, we see that $[\Sigma : K] = 5$, so that the Galois group of the extension is cyclic of order 5. We saw in class how to make an isomorphism between $\mathrm{Gal}(\Sigma : K)$ and the group of fifth roots of unity: we fix a root β of f and map $\sigma \in \mathrm{Gal}(\Sigma : K)$ to the ratio $\sigma(\beta)/\beta$, which is a fifth root of 1.

c. $K = \mathbf{F}_2$, $f(t) = t^3 + t + 1$.

The polynomial is evidently irreducible because it has no roots. Hence $[\Sigma : K]$ is divisible by 3. The Galois group $\mathrm{Gal}(\Sigma : K)$ is a subgroup of the group of permutations of the set of roots of f, and this set has at most 3 elements because f is a cubic. Hence $\mathrm{Gal}(\Sigma : K)$ can be only the alternating group $\mathbf{A}_3$ or the symmetric group $\mathbf{S}_3$. It's also a cyclic group because we're dealing with finite fields. Conclusion: it's $\mathbf{A}_3$, which is a cyclic group of order 3.

d. $K = \mathbf{F}_p$, $f(t) = (t^2 - 1)(t^2 - 2)\cdots(t^2 - (p-1))$.

The Galois group is trivial when $p = 2$, since then $f(t) = t^2 + 1 = (t+1)^2$. Assume now that p is odd. Then the Galois group is cyclic of order 2. Here's why: among the numbers from 1 to $p-1$, there are $(p-1)/2$ squares and $(p-1)/2$ non-squares, as we discussed on quite a few occasions. Let a be a non-square. Then every number between 1 and $p-1$ (viewed mod p) is either a square itself or is a times a square. Hence the splitting field of f is just $K(\sqrt{a})$, which is a quadratic extension of K. [The majority of you seemed to think that the order of the Galois group was something like $2^{(p-1)/2}$.]

e. $K = \mathbf{Q}$, $f(t) = t^5 - 10t + 5$. (You might want to show that this polynomial has exactly 3 real roots.)

The polynomial is irreducible (Eisenstein at 5). (If you failed to mention this, you lost points!) It is similar enough to polynomials that we studied in class that you should all know that the Galois group will be $\mathbf{S}_5$ if we can show that there are exactly two non-real roots. The polynomial is negative for very negative t and is positive at 0. Hence it has a negative real root. Its value at 1 is -4, so it has a root between 0 and 1. Because $f(t) \to \infty$ for t large and positive, there is a real root that's bigger than 1. Hence there are at least 3 real roots. The derivative has only two roots, so by Rolle's theorem the polynomial f cannot have more than 3 roots.

3. *Let $\zeta = e^{2\pi i/37}$, $\alpha = \zeta + \zeta^{10} + \zeta^{26}$. Use Galois theory to calculate the degree $[\mathbf{Q}(\alpha) : \mathbf{Q}]$.*

Let $L = \mathbf{Q}(\zeta)$. As we know from the course, $L : \mathbf{Q}$ is a Galois extension whose Galois group is naturally isomorphic to $(\mathbf{Z}/37\mathbf{Z})^*$. If $\sigma \in \mathrm{Gal}(L : \mathbf{Q})$ corresponds to $a \in (\mathbf{Z}/37\mathbf{Z})^*$, the $\sigma(\zeta) = \zeta^a$. It is traditional to write σ_a for this σ. If $G = \mathrm{Gal}(L : \mathbf{Q})$ and H is the group of $\sigma \in G$ such that σ is the identity on $\mathbf{Q}(\alpha)$, then Galois theory tells us that $[\mathbf{Q}(\alpha) : \mathbf{Q}]$ is the index of H in G. Note also that σ is the identity on $\mathbf{Q}(\alpha)$ if and only if σ is the identity on α. In terms of numbers $a \in (\mathbf{Z}/37\mathbf{Z})^*$, H is the group of those a such that

$$\zeta + \zeta^{10} + \zeta^{26} = \zeta^a + \zeta^{10a} + \zeta^{26a},$$

where the exponents are computed mod 37; we take them to be numbers between 1 and 36. Notice that ζ satisfies no non-zero polynomial of degree ≤ 36 other than multiples of its minimal polynomial, which has 37 terms. We thus have $\zeta + \zeta^{10} + \zeta^{26} = \zeta^a + \zeta^{10a} + \zeta^{26a}$ only when the three terms on the left coincide with the three terms on the right (possibly after re-ordering). In particular, the equation can be satisfied only when a is one of the three numbers 1, 10, 26. On the other hand, the equation is certainly satisfied when $a = 1$. When $a = 10$, $\zeta^a = \zeta^{10}$, $\zeta^{10a} = \zeta^{100} = \zeta^{26}$ (because $100 \equiv 26 \bmod 37$), and $\zeta^{26a} = \zeta^{260} = \zeta$ (because 260 is 1 mod 37). It is also satisfied when $a = 26$ for similar reasons. Alternatively, we can argue that H contains σ_{10} and therefore must contain $\sigma_{10}^2 = \sigma_{100}$. Since $100 \equiv 26 \bmod 37$, as we said, $\sigma_{100} = \sigma_{26}$. To summarize, H has order 3, and thus $(G : H) = 36/3 = 12$. The degree of $\mathbf{Q}(\alpha)$ over $\mathbf{Q}$ is 12.

4. *What does it mean to say that a finite extension of fields is separable? Construct a finite extension that is not separable, and explain in detail why the construction yields what is required.*

This is straightforward in the sense that you can look up the answer in our book. Briefly, $L : K$ is separable if, for each $a \in L$, the minimal polynomial of a over K is separable in the sense that it has no repeated roots in a splitting field for the polynomial. To make a non-separable, $L : K$, you have to take K to be an infinite field of characteristic p, where p is some prime. The example that we did in class had $L = k(x)$, where $k = \mathbf{F}_p$ and had $K = k(x^p)$, which is the image of L under the pth-power map $L \to L$.

5. *Suppose that G is a finite group. For each $g \in G$, let $S_g = \{\, xgx^{-1} \mid x \in G \,\}$. Show that the number of elements of S_g is a divisor of the order of G.*

As we discussed in class, there is a natural bijection $G/C(g) \xrightarrow{\sim} S_g$, where $C(g)$ is the centralizer of g, i.e., the group of elements of G that commute with g. The bijection maps a coset $xC(g)$ to the conjugate xgx^{-1} of g by x. (You have to check that this map is well defined and is indeed a bijection, but this is quite easy.) The cardinality of S_g is thus the index $(G : C(g))$, which is a divisor of the order of G.

6. *Suppose that $L : K$ is a finite Galois extension and that E is a subfield of L that contains K. Assume that L is the smallest subfield of L that contains E and is Galois over K (i.e., that no proper subfield of L has this property). Show that no proper subfield of L contains all the fields $\sigma(E)$ as σ runs over* $\mathrm{Gal}(L : K)$.

Let $G = \mathrm{Gal}(L : K)$ and let $H = \mathrm{Gal}(L : E) \subseteq G$. If F is a field between L and K, then F corresponds to a subgroup $I = \mathrm{Gal}(L : F)$ of G. To say that F is Galois over K is to say that I is normal in G. To say that F contains E is to say that I is contained in H. Thus the assumption of the problem amounts to the statement that $\{e\}$ is the only normal subgroup of G that is contained in H. Now suppose that F contains all $\sigma(E)$. What is $\mathrm{Gal}(L : F)$? If $\tau \in \mathrm{Gal}(L : F)$, then τ fixes $\sigma(E)$, so $\sigma\tau\sigma^{-1}$ fixes E. Since this is true for all σ, τ belongs to the intersection of all the conjugates of H in G. This intersection is a normal subgroup of G that is contained in H. By our assumption, it's the identity. Thus $\tau = \mathrm{id}$; it follows that $\mathrm{Gal}(L : F)$ is the identity subgroup of G, so that $F = L$ by Galois theory.