Math 306, Spring 2012
Final Exam Solutions

Name: ______________________________ Student ID: __________________________

Directions: Check that your test has 12 pages, including this one and the blank one on the bottom (which you can use as scratch paper or to continue writing out a solution if you run out room elsewhere). **Please show all your work**. **Write neatly: solutions deemed illegible will not be graded, so no credit will be given.** This exam is closed book, closed notes. You have 2.5 hours. Good luck!

1. (30 points) _____________

2. (11 points) _____________

3. (7 points) ______________

4. (10 points) _____________

5. (7 points) ______________

6. (12 points) _____________

7. (10 points) _____________

8. (7 points) ______________

9. (7 points) ______________

Total (out of 101): ______________

Curved exam score (out of 100): ______________

Course numerical grade_____________ **+ extra credit (out of 100):** ______________

Final course letter grade____________ **Final exam letter grade:** ______________

1. (3 pts each) Give brief answers to the following questions. No explanations are required unless otherwise indicated.

   (a) Give an example of a degree four polynomial over $\mathbb{Q}$ which is irreducible by Eisenstein Criterion.

   Solution: $x^4 + 2$

   (b) Give an example of a field of order 16 which is a quotient of $\mathbb{Z}_2[x]$.

   Solution: $\mathbb{Z}_2[x]/(x^4 + x^3 + x^2 + x + 1)$

   (c) Is it true that $*$ and $\dagger$ are always inverses of each other? Explain briefly or give a counterexample.

   Solution: No, see class notes.

   (d) Give an example of an extension $L\colon K$ such that $\text{Gal}(L/K) \cong \mathbb{Z}_3$

   Solution: This was a problem on the second midterm exam.

   (e) Give an example of a nontrivial Galois extension of $\mathbb{Q}$.

   Solution: $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$

   (f) Give an example of extensions $L\colon M$ and $M\colon K$ which are both Galois, but $L\colon K$ is not Galois.

   Solution: $K = \mathbb{Q}$, $M = \mathbb{Q}(\sqrt{2})$, $L = \mathbb{Q}(\sqrt[4]{2})$

   (g) Find an irreducible $f \in \mathbb{Q}[x]$ whose Galois group over $\mathbb{Q}$ is nonabelian.

   Solution: $x^3 - 2$ (Galois group is S_3)

   (h) Find all the subfields of $\mathbb{F}_{625}$. Note that $625 = 5^4$.

   Solution: $\{e\}$, $\mathbb{F}_5$, $\mathbb{F}_{25}$, $\mathbb{F}_{625}$

   (i) Is it true that the homology groups of any exact sequence are trivial? Explain briefly or give a counterexample.

   Solution: Yes, by definition the homology groups are computed by taking the kernel of a homomorphism modulo the image of the previous one. If a sequence is exact, then two are the same and the quotient is thus trivial.

   (j) Give an example of a functor from the category of sets to the category of groups.

   Solution: The functor which associates to a set the free group generated by the elements of that set.

2. (a) (6 pts) Define what it means for a field extension to be (i) simple, (ii) normal, and (iii) separable.

Solution: See book or notes.

(b) (5 pts) Suppose that $[L : K]$ is a prime number. Prove that $L : K$ is a simple extension.

Solution: This was a homework problem.

3. (7 pts) Show that Gal$(\mathbb{R}/\mathbb{Q})$ is the trivial group.

Solution: Since every positive element of $\mathbb{R}$ is a square, it follows that an automorphism of $\mathbb{Q}$ sends positives to positives. I.e. if a is negative and maps to $b > 0$ under an automorphism, then $\sqrt{b}$ must come from $\sqrt{c}$ which is not in $\mathbb{R}$. An automorphism σ therefore preserves the order in $\mathbb{R}$, so if $a < b$, $\sigma(a) < \sigma(b)$. Since any non-rational real number a can be trapped between rationals which are arbitrarily close to it, and since those rationals are sent to themselves, a thus must get sent to itself under σ. Therefore σ is the identity automorphism.

4. (5 pts each)

(a) If $[K(\alpha) : K]$ and $[K(\beta) : K]$ are relatively prime, show that $[K(\alpha, \beta) : K] = [K(\alpha) : K][K(\beta) : K]$.

Solution: See class notes.

(b) Let p be a prime and let a be a rational number which is not a p-th power of another rational number. Let L be the splitting field of $x^p - a \in \mathbb{Q}[x]$. Prove that L is obtained by adjoining a pth real root α of a and a primitive pth root of unity ζ to $\mathbb{Q}$. Also prove that $[L : \mathbb{Q}] = p(p-1)$.

Solution: See class notes and second midterm.

5. (7 pts) Construct the subfield and subgroup lattice diagrams related to the Galois group of $x^4 - 12x^2 + 35 \in \mathbb{Q}[x]$.

Solution: This was a homework problem.

6. (12 pts) State all five parts of the Fundamental Theorem of Galois Theory. Prove any three of the five parts, stating carefully any other theorems of lemmas you are using (which you do not need to prove).

   Solution: See class notes.

7. (a) (5 pts) Show that any finite field must have p^n elements, where p is prime and $n \in \mathbb{N}$.

Solution: See class notes.

(b) (5 pts) Show that, given $\mathbb{F}_{p^n}$ and $d \in \mathbb{N}$, there exists an irreducible polynomial $f \in \mathbb{F}_{p^n}[x]$ of degree d.

Solution: See class notes.

8. (7 pts) Suppose the diagram

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "f"] \arrow[d, "\alpha"] & B \arrow[r, "g"] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & A' \arrow[r, "f'"] & B' \arrow[r, "g'"] & C' \arrow[r] & 0
\end{tikzcd}$$

of abelian groups commutes and the rows are exact. Show that if α and γ surjections, then so is β. (This is a part of the *Short Five Lemma*.)

Solution: Given $b' \in B'$, we want to show that there exists an element in B which maps to it under β. Since g and γ are surjections (by exactness of the top row and assumption, respectively), there exists a $b \in B$ such that $\gamma(g(b)) = g'(b')$. Since the right square commutes,

$$\gamma(g(b)) = g'(\beta(b)) = g'(b').$$

Since $\beta(b)$ and b' both map to the same element under g', it must be that $g'(b' - \beta(b)) = 0$. Thus $b' - \beta(b) \in \ker g'$ and, by exactness of the bottom row, there thus exists $a' \in A'$ such that $f'(a') = b' - \beta(b)$. By assumption, α is a surjection, so there exists $a \in A$ such that $\alpha(a) = a'$. So

$$b' - \beta(b) = f'(a') = f'(\alpha(a)).$$

By commutativity of the left square, $\beta(f(a)) = f'(\alpha(a))$ and so $b' - \beta(b) = \beta(f(a))$. But then $\beta(f(a)) + \beta(b) = b'$, or $\beta(f(a) + b) = b'$ and we have thus found an element in B' which maps to b'.

9. (a) (3 pts) Write down the precise definition of a category.

Solution: See class notes.

(b) (4 pts) Show that any group G can be regarded as a category with one object and one morphism for each element of G.

Solution: See class notes.