Math 306, Spring 2008
Final Exam Preparation

Your final exam is self-scheduled and can be taken any time during the finals period. It is a closed-notes, closed-book, open-brain, no-calculator 2.5-hour examination. The exam is cumulative, and will have the same format as the midterms except it will be roughly twice as long. Later material will be emphasized more heavily.

What follows are some guidelines for studying the portion of the material covered since the second midterm. To study for earlier topics, use review handouts for first and second midterms.

How to study for the exam

The exam will be friendly to those who have studied carefully and followed all the instructions on this sheet. Most of the test questions will look familiar. You will be asked to repeat some definitions, state some theorems, and reproduce some proofs you have seen before. The exam will contain some exercises you have not seen before, but they will not comprise the bulk of the exam.

(1) Read this worksheet thoroughly.
(2) Read and understand your class notes.
(3) Know how to do all the homework problems. You already have the solutions to all of them.
(4) Go to office hours to ask questions.
(5) After you have done all of the above, start on the review problems at the end of this handout.

What you need to commit to memory

(1) You must know the definitions of the following.

(a) Galois extension
(b) Frobenius map
(c) Exact sequence
(d) Short exact sequence
(e) Split extension
(f) Free group, presentation of a group
(g) Free resolution
(h) Complex
(i) Homology groups of a complex
(j) Category
(k) Functor
(l) Natural transformation

(2) You must know the statements and proofs (unless otherwise indicated) of the following.

(a) Theorems 10, 11 (ok to assume Lemmas A and B), 12, 13, 14, 15, 16, 17 (statement only), 18, 19 (the big one!)
(b) A finite field must have p^n elements
(c) Any subgroup of $K^\times$ is cyclic if K finite (statement only)
(d) K is a finite field with p^n elements iff K is a splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$ (statement only)
(e) Any finite field is a simple extension of $\mathbb{Z}_p$ (statement only)
(f) Any two fields with p^n elements are isomorphic
(g) $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \iff m|n$ (statement only for $\Leftarrow$)
(h) There exists an irreducible polynomial of degree d in $\mathbb{F}_{p^n}[x]$ for any d
(i) The Frobenius map is a $\mathbb{Z}_p$-automorphism (statement only)
(j) The Galois group of a finite extension of a finite field is cyclic
(k) Splitting Lemma (statement only)
(l) Short Five Lemma

Topics you must study

(1) Finding Galois groups and using $*$ and $\dagger$ to go back and forth between subgroups of the Galois groups and intermediate fields
(2) Using the Fundamental Theorem of Galois Theory
(3) Finite fields
(4) Exact sequences and their applications
(5) Free groups and presentations of groups
(6) Categories and functors

Computational problems you must be able to do

(1) Verifying that an extension is Galois
(2) Computing the Galois group of an extension or of a polynomial (listing all automorphisms – and arguing that there are no more – and studying their properties to conclude what the group structure is)
(3) Figuring out lattice diagrams of subgroups of the Galois group and intermediate fields
(4) Finding presentations of groups
(5) Verifying a sequence of groups and homomorphisms is exact
(6) Computing homology of simple complexes
(7) Verifying that something is a category or a functor between categories

Summary of Theorems 1–19

(1) Theorems 1 and 2 say that the adjoining of different roots of the same minimum polynomial gives isomorphic field extensions.
(2) Theorems 3 and 4 say that splitting fields of polynomials (irreducible or not) are unique.
(3) Theorem 5 characterizes finite normal extensions.
(4) Theorem 7 tells us that automorphisms are determined precisely by their behavior on the roots of the relevant irreducible polynomials.
(5) We skipped Theorems 8 and 9.
(6) Theorem 11 gives our first numerical relationship between subgroups of the Galois group and their fixed fields.
(7) Theorem 14 gives a numerical result that illuminates the importance of separability.
(8) Theorem 15 is the first major theorem.
(9) Theorems 16 and 18 are converses of each other, giving an alternate way of thinking about Galois extensions.
(10) Theorem 19 gives the one-to-one correspondence between the subgroups of the Galois group and the intermediate subfields of the extension. It also gives the relationship between normal subgroups and normal field extensions.

Review Problems (solutions will be provided later)

Note: For practice with exact sequences and category theory use the last homework.

(1) Let α denote the positive fourth root of 2. Find the Galois group of x^4+2 over each of the fields: (i) $\mathbb{Q}(\sqrt{2})$, (ii) $\mathbb{Q}(\sqrt{2},i)$, (iii) $\mathbb{Q}(\alpha)$, (iv) $\mathbb{Q}(\alpha,i)$.

(2) Find an extension L of $\mathbb{Q}$ such that $\mathrm{Gal}(L/\mathbb{Q})$ is isomorphic to (a) $\mathbb{Z}_4$, (b) $\mathbb{Z}_6$, (c) $S_3\times\mathbb{Z}_{10}$.

(3) (a) Give an example of a field K and two nonisomorphic extensions L_1 and L_2 such that $\mathrm{Gal}(L_1/K)\cong\mathrm{Gal}(L_2/K)$.
(b) Let $L\colon K$ be a finite extension. Prove that $\mathrm{Gal}(L/K)$ is a finite group. Give examples to show that, if $L\colon K$ is infinite, then the Galois group may either be finite or infinite.

(4) Let L be a Galois extension of K such that $\mathrm{Gal}(L/K)\cong\mathbb{Z}_2\times\mathbb{Z}_{12}$. How many intermediate fields M are there such that (i) $[L\colon M]=4$, (ii) $[L\colon M]=9$, (iii) $\mathrm{Gal}(L/M)\cong\mathbb{Z}_4$?

(5) Let $K\subseteq M\subseteq L$ be fields. Prove or disprove.
(a) If $L\colon K$ is Galois, then $L\colon M$ is Galois.
(b) If $L\colon K$ is Galois, then $M\colon K$ is Galois.
(c) If $M\colon K$ and $L\colon M$ are Galois, then $L\colon K$ is Galois.

(6) Find the Galois group of x^4-2 over (i) $\mathbb{Z}_3$ and (ii) $\mathbb{Z}_7$.

(7) (a) Using the fact that $\mathbb{F}_{p^n}\colon\mathbb{Z}_p$ is always Galois, show that, if $f\in\mathbb{Z}_p[x]$ is irreducible, then $\mathbb{Z}_p(\alpha)$ is the splitting field for f for any root α of f.
(b) Prove that, if $f\in\mathbb{F}_{p^m}[x]$ is irreducible, then f divides $x^{p^{mn}}-x$ iff the degree of f divides n.

(8) Let p and q be prime numbers. Prove that there are $\frac{p^{mq}-p^m}{q}$ irreducible polynomials $f\in\mathbb{F}_{p^m}[x]$ of degree q. (Hint: Use the previous problem.)