Math 306, Spring 2012
Midterm 2 Preparation

Your second midterm is on Thursday, April 12. It is a closed-note, closed-book, open-brain, no-calculator 70-minute examination held during the regular class time. It will cover up to and including the material that appeared on Homework 8.

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 and quiz problems. The solutions are on our class conference.
(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) Constructible points
- (b) What it means for f to split over a field
- (c) Splitting field
- (d) Normal extension
- (e) Normal closure
- (f) Separable polynomial, element, extension
- (g) Formal derivative of a polynomial
- (h) K-monomorphism, K-automorphism of an extension $L : K$
- (i) Galois group of $L : K$
- (j) Maps $*$ and $\dagger$
- (k) Fixed field

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

- (a) Statement that $\pi/3$ cannot be trisected using ruler and compass
- (b) Lemma that $[K(\alpha, \beta) : K] = [K(\alpha) : K][K(\beta) : K]$ if $gcd(m, n) = 1$
- (c) Theorems 1,2, 5 (you were assigned to read the proof of Theorem 5 on your own)
- (d) Theorems 3,4 (statements only)
- (e) Statement that $f \in [x]$ has a repeated root in an extension L of K iff f and Df have a common root.
- (f) Galois Correspondence (statement only; this is part 2. of Theorem 19 and we'll prove it later)
- (g) Theorems 6, 7
- (h) Theorems 11, 14, 15 (statements only)

Topics you must study

(1) (In)constructibility
(2) Splitting fields
(3) Normal extensions
(4) Normal closures
(5) Separability
(6) Formal differentiation and how it behaves over fields with different characteristics
(7) Galois group
(8) Galois correspondence (properties of maps $*$ and $\dagger$)
(9) K-monomorphisms

Computational problems you must be able to do

(1) Finding the splitting field for a polynomial and the degree of the splitting extension
(2) Finding a normal extension (or verifying an extension is normal) and finding its degree
(3) Finding a normal closure and its degree
(4) Verifying a polynomial is separable in a given field or finding one where it is
(5) Manipulating the formal derivative of a polynomial
(6) 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)
(7) Computing fixed fields of the subgroups of the Galois group

Review Problems (solutions will be provided later)

(1) Determine the splitting field and degree over $\mathbb{Q}$ for the following polynomials.
  (a) $x^4 + x^2 + 1$
  (b) $x^4 + 4$
  (c) $x^6 + x^3 + 1$
  (d) $x^6 + 1$

(2) Let K be a field.
  (a) Let $a, b \in K$ and $a \neq 0$. Consider the map $\phi\colon K[t] \to K[t]$ defined by $\phi(f) = f(at + b)$. Prove that ϕ is a K-automorphism of $K[t]$.
  (b) Conversely, let ϕ be a K-automorphism of $K[t]$. Prove that there are $a, b \in K$ with $a \neq 0$ such that $\phi(f) = f(at + b)$. (Hint: Show that $\deg \phi(t)$ must be 1 by contradiction.)

(3) Consider the extension $K\colon F$ and let $\phi\colon K \to K'$ be an isomorphism. Suppose that $\phi(F) = F'$.
  (a) If $\sigma \in \mathrm{Gal}(K/F)$, prove that $\phi\sigma\phi^{-1}$ lies in $\mathrm{Gal}(K'/F')$.
  (b) Prove that the map $\psi\colon \mathrm{Gal}(K/F) \to \mathrm{Gal}(K'/F')$, defined by $\psi(\sigma) = \phi\sigma\phi^{-1}$, is a group isomorphism.

(4) (a) Suppose that $\operatorname{char} K = p \neq 0$. Consider the map $\phi\colon K \to K$ given by $\phi(\alpha) = \alpha^p$ for all $\alpha \in K$. Prove that ϕ is a ring monomorphism. This mapping is called the *Frobenius monomorphism*.
  (b) Suppose that $\operatorname{char} K = p > 0$. Prove that K is perfect (i.e. every polynomial in $K[x]$ is separable) iff the Frobenius monomorphism is an automorphism.

(5) Let $n \in \mathbb{Z}_{\geq 3}$ and let $f = x^n - 1 \in \mathbb{Q}[x]$. If L is the splitting field for n, prove that $\mathrm{Gal}(L/\mathbb{Q})$ is abelian. (Hint: show that an element $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ must send $e^{2\pi i/n}$ to $e^{2\pi ik/n}$ for some $k \in \mathbb{Z}$ and σ is determined by $e^{2\pi i/n} \mapsto e^{2\pi ik/n}$.)

(6) Let $L\colon K$ be a field extension. Let H be a subgroup of $\mathrm{Gal}(L/K)$ and M be an intermediate subfield. Prove that $H \subseteq H^{\dagger *}$.

(7) For each of the following extensions $L\colon K$, find (i) $\mathrm{Gal}(L/K)$, (ii) $H^\dagger$ for all the subgroups H of $\mathrm{Gal}(L/K)$,
  (a) $\mathbb{Q}(\sqrt{1+\sqrt{3}})\colon \mathbb{Q}$
  (b) $L\colon \mathbb{Z}_2$, where L is the splitting field of $x^2 + x + 1 \in \mathbb{Z}_2[x]$
  (c) $L\colon \mathbb{Z}_5$, where L is the splitting field of $(x^2 - 2)(x^2 - 3) \in \mathbb{Z}_5[x]$
  (d) $L\colon \mathbb{Z}_7$, where L is the splitting field of $x^3 - 5 \in \mathbb{Z}_7[x]$
  (e) $L\colon \mathbb{Z}_5$, where L is the splitting field of $(x^5 - t)(x^5 - u) \in \mathbb{Z}_5(t, u)[x]$, where t is transcendental over $\mathbb{Z}_5$ and u is transcendental over $\mathbb{Z}_5(t)$