Math 306, Spring 2012
Midterm 1 Preparation

Your first midterm is on Thursday, March 8. 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 5.

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 review handout.

What you need to commit to memory

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

- (a) Ring, subring, field, subfield
- (b) Polynomial ring
- (c) Ring/field homomorphism and isomorphism
- (d) Kernel
- (e) Ideal
- (f) Quotient ring
- (g) Principal ideal, principal ideal domain
- (h) Characteristic of a ring
- (i) Integral domain
- (j) Field of fractions
- (k) Highest common factor of two polynomials
- (l) Irreducible polynomial
- (m) Unique factorization domain
- (n) Root (zero) of a polynomial
- (o) Field extension
- (p) Subfield generated by a subset
- (q) Simple extension
- (r) Algebraic and transcendental elements
- (s) Minimal polynomial
- (t) (Primitive) root of unity
- (u) Cyclotomic polynomial/extension
- (v) Degree of an extension

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

- (a) Statement that $\mathbb{Z}/\mathbb{Z}_n$ is a field iff n is a prime
- (b) Statement that F is a field $\Longrightarrow F$ is an integral domain
- (c) Statement that R is an integral domain $\Longrightarrow R[x]$ is an integral domain
- (d) First Isomorphism Theorem for Rings (statement only)
- (e) Division Algorithm (statement only)
- (f) Statement that if $d(x)$ is a highest common factor of $f(x)$ and $g(x)$, so is $kd(x)$ for any $k \in K$, where K is the ground field
- (g) Euclidean Algorithm (statement only)
- (h) Statement that polynomials over a field factor uniquely up to constant multiples and reordering (just read the outline of proof in your notes)
- (i) Gauss' Lemma
- (j) Eisenstein Criterion
- (k) Statement that α is a root of f iff $x - \alpha$ divides f (statement only)

(l) Statement that if α is algebraic over K then the minimal polynomial of α is irreducible over K and it divides every other polynomial which has α as a zero

(m) Statement that there is an isomorphism between $K[x]/(m)$ and $K(\alpha)$ where α is algebraic over K and m is its minimal polynomial

(n) Statement that roots of unity form a cyclic group generated by any primitive root of unity

(o) Tower Law

(p) Statement that $K(\alpha) : K$ is finite $\Leftrightarrow$ α is algebraic over K (statement only)

Topics you must study

(1) Examples of rings and fields: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $R[x]$, Gaussian integers, $n\mathbb{Z}$, $\mathbb{Z}/\mathbb{Z}_n$, $R \times S$, R^S, quotient rings, fields of fractions, $K(\alpha)$

(2) Ring homomorphisms and isomorphisms

(3) PIDs, integral domains

(4) Division of polynomials, highest common factor, Euclidean Algorithm

(5) Showing irreducibility

(6) Gauss' Lemma

(7) Eisenstein Criterion

(8) Field extensions

(9) Subfields generated by adjoining elements

(10) Simple extensions

(11) Algebraic extensions

(12) Minimal polynomials

(13) Constructing fields of order p^n, p prime

(14) Roots of unity

Computational problems you must be able to do

(1) Verifying something is a (sub)ring or a (sub)field

(2) Verifying a map is a homomorphism or an isomorphism

(3) Finding a field of fractions

(4) Finding the quotient and remainder using Division Algorithm

(5) Showing polynomial is (ir)reducible (by contradiction after supposing there is, Gauss' Lemma, Eisenstein Criterion, or by finding zeros)

(6) Showing a ring is or isn't a UFD

(7) Writing out explicitly what elements of an extension look like

(8) Showing that an extension is simple

(9) Finding minimal polynomials

(10) Finding fields of order p^n for p prime

(11) Finding (primitive) roots of unity

Review Problems (solutions will be provided later)

(1) (a) Let R be an integral domain. Prove that the set $U(R)$ of units of R is an abelian multiplicative group.
(b) Prove that, if K is a field, then $K[x,y]$ is not a principal ideal domain.

(2) Let R be a ring and let x and y be indeterminates. Recall that $R[x,y]$ can be thought of as $(R[x])[y]$. It is easy to see that $R[x,y] \cong R[y,x]$. By induction we can define $R[x_1,\dots,x_n]$ where the x_i are all indeterminates. Let $p = 2x^2y - 3xy^3z + 4y^2z^5$ and $q = 7x^2 + 5x^2y^3z^4 - 3x^2z^3$ be elements in $\mathbb{Z}[x,y,z]$.
(a) Write p and q as polynomials in x with coefficients in $\mathbb{Z}[y,z]$. Find the degrees of p and q.
(b) Write p and q as polynomials in y with coefficients in $\mathbb{Z}[x,z]$. Find the degrees of p and q.

(3) Prove that $\mathbb{Q}[x,y]$ is not a PID.

(4) Find the quotient and the remainder upon division of x^3 by x^2+x+1 in $\mathbb{Z}_2[x]$.

(5) (a) Prove that $x^4+4x^3+6x^2+2x+1$ is irreducible in $\mathbb{Q}[x]$.
(b) Find all the complex roots of $f = x^4+3$. Find the smallest field L containing $\mathbb{Q}$ such that f completely factors into linear polynomials in $L[x]$. (Hint: the required L will satisfy $[L\colon \mathbb{Q}] = 8$.)

(6) (a) Let $n \in \mathbb{Z}_{\geq 2}$ and suppose that $a_nx^n + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$ has a factor $ax+b$. Show $a|a_n$ and $b|a_0$.
(b) Suppose α is a rational root of a monic polynomial in $\mathbb{Z}[x]$. Prove that α is an integer.

(7) Describe the subfields of $\mathbb{C}$ of the form $\mathbb{Q}(\sqrt{5},\sqrt{7})$ and $\mathbb{Q}(e^2+1)$. Write the first in the form $\mathbb{Q}[x]/(m)$ where m is an irreducible polynomial.

(8) Let $\mathbb{A}$ be the collection of all $\alpha \in \mathbb{C}$ such that α is algebraic over $\mathbb{Q}$.
(a) Prove that, if $\alpha \in \mathbb{A}^*$, then $\alpha^{-1} \in \mathbb{A}$.
(b) Prove that, if $\alpha, \beta \in \mathbb{A}$, then $\alpha - \beta$ and $\alpha\beta$ belong to $\mathbb{A}$.
(c) Conclude that $\mathbb{A}$ is a field.
(Hint: Recall that, if $K(\alpha)\colon K$ is finite, then α is algebraic over K.)

(9) Let K be a field and let x be an indeterminate. Denote by $K(x)$ the field of fractions of $K[x]$. Let $t = p/q \in K(x)$, where p and q are coprime polynomials in $K[x]$ and $q \neq 0$.
(a) Is $K(x)$ an extension of $K(t)$, or is $K(t)$ an extension of $K(x)$? Explain.
(b) Prove that $f = p - tq \in K(t)[x]$ is irreducible over $K(t)$.
(c) Prove that $[K(x)\colon K(t)] = \max\{\deg p, \deg q\}$.

(10) Determine, with explanation, whether the following are true or false.
(a) Every field has a nontrivial extension.
(b) Every field has a nontrivial algebraic extension.
(c) Every simple extension is algebraic.
(d) Every root of unity is algebraic over $\mathbb{Q}$