MATH 100B – Midterm Study Guide

Alina Bucur

First, let me warn you that this is by no means a complete list of problems, or topics. Just highlights. The first thing you should do when preparing for the exam is to go through your notes, the relevant sections of the book and the homework problems for HW1-4. If you still have trouble with some of the topics encountered so far, take the book (or another abstract algebra book) and solve more problems related to that topic until you really understand how and why things work. The quiz will cover sections 3.1-3.4 and 4.1-4.3.
You will have 11-11:50 (the whole lecture) to do the quiz. Please be on time!

Topics

rings: definition, examples
subrings, ideals, maximal ideals, prime ideals, quotient rings
homomorphisms of rings, isomorphisms of rings, kernel, image
product of rings, ideals in product of rings and quotient rings
isomorphism theorems
nilpotents, zero divisors, group of units in a ring, annihilators
integral domains, fields, subfields, field of fractions of an integral domain
division rings, simple rings
characteristic of a ring, center of a ring
gaussian integers, $\mathbb{Q}(i)$, $\mathbb{Z}[\sqrt{d}]$ and $\mathbb{Q}(\sqrt{d})$
The Chinese Remainder Theorem
the ring of polynomials over a commutative ring
polynomials over a field: long division, irreducibles, unique factorization, quotient rings
recall that $\mathbb{F}_p$ denotes the finite field with $p$ elements, namely $\mathbb{Z}/p\mathbb{Z}$

Practice problems

This is a collection of problems to help you prepare for the midterm. Once again, the list is not complete and these problems do not imply anything about the content of the test.

1. Go over HW.
2. Section 3.3: 21, 33, 35
3. Let $R$ be a ring and $I, J$ ideals in $R$. Prove that
   (a) $I + J, I \cap J$ and $IJ$ are ideals in $R$.
   (b) $IJ \subseteq I \cap J$.
   (c) $I \cap J$ is the biggest ideal of $R$ contained in both $I$ and $J$.
   (d) $I + J$ is the smallest ideal of $R$ that contains both $I$ and $J$.
4. Show that a finite integral domain is a field.
5. Let $P$ be a prime ideal in the commutative ring $A$. Let $S = A \setminus P$ the complement of $P$ in $A$. 

1
(a) Prove that if $a \in S$ and $b \in S$, then $ab \in S$. ($S$ is a multiplicatively closed subset of $A$.)

(b) Prove that $1 \in S$.

(c) Prove that
\[(a, s) \sim (b, t) \iff u(at - bs) = 0 \text{ for some } u \in S\]
defines an equivalence relation on $A \times S$.

(d) Denote by $A_P$ the set of equivalence classes $\frac{a}{s}$ of $A \times S$ with respect to the equivalence relation defined in (b). Prove that $A_P$ is a ring with respect to
\[\frac{a}{s} + \frac{b}{t} = \frac{a + bs}{st}\]
and
\[\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.
\]
You do need to worry about the operations being well-defined. What are $0_{A_P}$ and $1_{A_P}$?

$A_P$ is called the localization of $A$ at the prime ideal $P$.

(e) Prove that $f : A \to A_P$ given by $f(a) = \frac{a}{1}$ is a ring homomorphism and compute its kernel.

(f) What is $A_P$ when $A = \mathbb{Z}$ and $P = 0$?

(g) What is $A_P$ when $A = \mathbb{Z}$ and $P = 2\mathbb{Z}$?

(h) What is $A_P$ when $A = \mathbb{Z}[X]$ and $P = \text{Ap}(X)$ where $p(X) = X + 1$?

6. The construction above works more generally. Suppose $A$ is a commutative ring and $S \subset A$ is a subset with the property that if $s, t \in S \implies st \in S$ for any $s, t \in A$ and such that $0 \notin S$ and $1 \in S$.

(a) Prove that
\[(a, s) \sim (b, t) \iff u(at - bs) = 0 \text{ for some } u \in S\]
defines an equivalence relation on $A \times S$.

(b) Denote by $S^{-1}A$ the set of equivalence classes $\frac{a}{s}$ of $A \times S$ with respect to the equivalence relation defined in (a). Prove that $S^{-1}A$ is a commutative ring with respect to
\[\frac{a}{s} + \frac{b}{t} = \frac{a + bs}{st}\]
and
\[\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.
\]
You do need to worry about the operations being well-defined. What are $0_{S^{-1}A}$ and $1_{S^{-1}A}$?

(c) Prove that $f : A \to A_P$ given by $f(a) = \frac{a}{1}$ is a ring homomorphism.

(d) Assume $B$ is a commutative ring and $g : A \to B$ is a ring homomorphism such that $g(s) \in U(B)$ for all $s \in S$. Show that there exist a unique ring homomorphism $h : S^{-1}A \to B$ such that $h \circ f = g$.

7. Let $A$ be a commutative ring and fix an element $a \in A$. Prove that the map $\varphi : A[X] \to A$ given by $\varphi(f(X)) = f(a)$ is a ring homomorphism. Find its kernel and image.

8. Let $f : R \to S$ be a ring homomorphism.
(a) Show that if $J$ is an ideal in $S$ then

$$f^{-1}(J) = \{ a \in R; f(a) \in J \}$$

is an ideal in $R$ that contains ker $f$.

(b) If $f$ is surjective, show that the map $J \mapsto f^{-1}(J)$ is a bijection between the ideals of $S$ and the ideals of $R$ that contain ker $f$ that preserves primality and maximality for ideals.

9. You have proved in the homework that the ideals in a product of rings $R \times S$ are given by the $A \times B$ where $A$ is an ideal in $R$ and $B$ is an ideal of $S$. The corresponding statement is true for finite products of rings, but not for arbitrary products of rings. Find a counterexample for arbitrary products of rings. That is, find a family $\{ R_i \}_{i \in I}$ of rings (it will have to be infinite) and an ideal in

$$\prod_{i \in I} R_i = \{(a_i)_{i \in I}; a_i \in R_i \text{ for all } i \in I\}$$

that is cannot be written as a product $\prod_{i \in I} J_i$ of ideals $J_i$ of $R_i$ for each $i \in I$.

10. Let $d \in \mathbb{Z}$ be a square-free integer. Define $N : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}$ by $N(x + y\sqrt{d}) = x^2 - dy^2$.

(a) Show that $N(\alpha \beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$.

(b) Show that $N(\alpha) \in \mathbb{Z}$ if $\alpha \in \mathbb{Z}[\sqrt{d}]$.

(c) If $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$ we say that $\alpha | \beta$ (divides) if there exits an element $\gamma \in \mathbb{Z}[\sqrt{d}]$ such that $\beta = \alpha \gamma$. Show that

$$\alpha | \beta \implies N(\alpha) | N(\beta).$$

(d) Show that for $\alpha \in \mathbb{Z}[\sqrt{d}]$ we have

$$\alpha \in U(\mathbb{Z}[\sqrt{d}]) \iff N(\alpha) = \pm 1.$$

(e) Compute the group of units in $\mathbb{Z}[\sqrt{d}]$ for $d = -1, -2, -3$.

11. Let

$$\omega = \frac{-1 + i\sqrt{3}}{2} = \frac{-1 + \sqrt{-3}}{2}$$

and let

$$A = \mathbb{Z}[\omega] = \{ m + n\omega; m, n \in \mathbb{Z} \}$$

$$F = \mathbb{Q}(\omega) = \{ x + y\omega; x, y \in \mathbb{Q} \}$$

(a) Show that for any $x, y \in \mathbb{Q}$

$$(x + y\omega)(x + y\bar{\omega}) = x^2 - xy + y^2 = zz$$

where $z = x + y\omega$.

(b) Show that the map $N : F \to \mathbb{Q}$ given by $N(x + y\omega) = x^2 - xy + y^2$ for all $x, y \in \mathbb{Q}$ is well defined.

(c) Show that $N(\alpha \beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in F$.

(d) Show that $N(\alpha) \in \mathbb{Z}$ if $\alpha \in A$.

(e) If $\alpha, \beta \in A$ we say that $\alpha | \beta$ (divides) if there exits an element $\gamma \in A$ such that $\beta = \alpha \gamma$. Show that

$$\alpha | \beta \implies N(\alpha) | N(\beta).$$
22. Assume \( f \in A \) we have
\[
\alpha \in U(A) \iff N(\alpha) = \pm 1.
\]

23. Prove or disprove:
(a) \( \mathbb{Z}[X]/(X^2) \) is a local ring.
(b) \( \mathbb{Q}[X]/(X^2) \) is a local ring.
(c) \( \mathbb{R}[X]/(X^2) \) is a local ring.
(d) \( K[X]/(X^2 - 2) \) is a local ring where \( K = \mathbb{Q}(i) \).
(e) \( A[X]/(X^2 - 2) \) is a local ring where \( A = \mathbb{Z}(i) \).