MATH 100B – Final exam 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. 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 exam is cumulative. Please bring a blue book to the final.

This is a collection of problems to help you prepare for the final. 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) $IJ \subset I \cap J$.
   (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.
   (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
   $$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}$$
   and
   $$\frac{a}{s} + \frac{b}{t} = \frac{ab}{st}.$$
   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 $P = Ap(X)$ 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

$$s, t \in S \implies st \in S \text{ for any } s, t \in A$$

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

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}$$

and

$$\frac{a}{s} + \frac{b}{t} = \frac{ab}{st}.$$

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 $\alpha \mid \beta$ (divides) if there exits an element $\gamma \in \mathbb{Z}[\sqrt{d}]$ such that $\beta = \alpha\gamma$. Show that

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

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

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

(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 $x, y \in \mathbb{Q}$

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

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 $\alpha \mid \beta$ (divides) if there exits an element $\gamma \in A$ such that $\beta = \alpha\gamma$. Show that

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

(f) Show that for $\alpha \in A$ we have

$$\alpha \in U(A) \iff N(\alpha) = \pm 1.$$

(g) Compute the group of units in A.

12. A *local ring* is a commutative ring that has exactly one maximal ideal. Assume A is a commutative ring. Prove that the following are equivalent.

(a) A is a local ring.

(b) If $a, b \in A$ with $a + b = 1$ then $a \in U(A)$ or $b \in U(A)$.

(c) The set $M = A \setminus U(A)$ is an ideal in A.

13. Let $A = \mathbb{R}[X]$, $p(X) = X^2 + 1 \in A$ and $I = Ap(X)$. Prove that $\varphi : A/I \to \mathbb{C}$ given by $\varphi(f) = f(i)$ is a ring isomorphism.

14. Let $A = \mathbb{Q}[X]$, $p(X) = X^2 - 2 \in A$ and $I = Ap(X)$. Prove that $\varphi : A/I \to \mathbb{Q}(\sqrt{2})$ given by $\varphi(f) = f(\sqrt{2})$ is a ring isomorphism.

15. If m, n are two relatively prime positive integers, show that $\mathbb{Z}_{mn}$ and $\mathbb{Z}_m \times \mathbb{Z}_n$ are isomorphic rings. Find an isomorphism between them and prove that it is an isomorphism.

16. Find the gcd of $X^4 + X + 1$ and $X^3 + 1$ in $\mathbb{R}[X], \mathbb{C}[X], \mathbb{F}_3[X], \mathbb{F}_5[X]$.

17. Are the following polynomials irreducible? Justify your answer. If not, factor them into irreducibles.
    (a) $X^3 - X + 1$ in $\mathbb{Q}[X]$, $\mathbb{F}_7[X]$.
    (b) $X^4 + 1$ in $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{F}_{13}[X]$.
18. Show that $\mathbb{R}[X]/(X^2+1)$ is isomorphic to $\mathbb{C}$. Exhibit an isomorphism.
19. Show that $\mathbb{F}_3[X]/(X^2+1)$ is a field with 9 elements. Here (X^2+1) denotes the principal ideal of $\mathbb{F}_3[X]$ generated by the polynomial X^2+1.
20. Assume $f(X) \in \mathbb{F}_p[X]$ is an irreducible polynomial of degree n.
    (a) Show that the principal ideal $(f(X))$ of of $\mathbb{F}_p[X]$ generated by the element $f(X)$ is a maximal ideal.
    (b) Show that $\mathbb{F}_p[X]/(f(X))$ is a field with p^n elements. Give a description of the residue classes.
    (c) If $g(X) \in \mathbb{F}_p[X]$ is also an irreducible polynomial of degree n, construct an isomorphism of fields
    $$\varphi : \mathbb{F}_p[X]/(f(X)) \to \mathbb{F}_p[X]/(g(X))$$
    such that $\varphi(a) = a$ for all $a \in \mathbb{F}_p$.
21. 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 $A = \mathbb{Z}(i)$.
22. Prove that the following pairs of rings are not isomorphic.
    (a) $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-2}]$.
    (b) $\mathbb{F}_2[X]/(X^3+X)$ and $\mathbb{F}_2[X]/(X^3+X+1)$.
    (c) $\mathbb{R}$ and $\mathbb{C}$.
23. Define the elements $x = 9 + 20i$, $y = 13 - 4i$ in $\mathbb{Z}[i]$.
    (a) Use the Euclidean algorithm to compute the greatest common divisor of x and y in $\mathbb{Z}[i]$.
    (b) Find the prime factorizations of x and y in $\mathbb{Z}[i]$. Justify that your factors are indeed prime.
24. In each case, find one isomorphism between the following pairs of finite fields, and state the common order of the two fields.
    (a) $\mathbb{F}_5[X]/(X^2-2)$ and $\mathbb{F}_5[X]/(X^2-3)$.
    (b) $\mathbb{F}_2[X]/(X^3+X+1)$ and $\mathbb{F}_2[X]/(X^3+X^2+1)$.
25. Find the splitting field of $X^3 - 1$ over $\mathbb{Q}$.
26. Find the splitting field of $f(X) = X^3 - 2$ over the following fields.
    (a) $\mathbb{Q}$
    (b) $\mathbb{Q}(i)$
    (c) $\mathbb{F}_5$
    (d) $\mathbb{F}_7$.

27. Which of the following rings are euclidean? Which ones are PIDs? Which ones are UFDs?

$$\mathbb{Z}, \quad \mathbb{Z}[i], \quad \mathbb{Z}[\sqrt{-5}], \quad \mathbb{Z}[\sqrt{-3}], \quad \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$$

28. State and prove the Eisenstein Criterion.

29. Find the $\mathrm{Aut}(K/F)$ for the following field extensions.

    (a) $\mathbb{C}/\mathbb{R}$
    (b) $\mathbb{Q}(i)/\mathbb{Q}$
    (c) $\mathbb{F}_{25}/\mathbb{F}_5$
    (d) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$
    (e) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$
    (f) $K/\mathbb{Q}$ where K is the splitting field of $X^3 - 2 \in \mathbb{Q}[X]$.

30. Define the elements $x = 9 + 20i$, $y = 13 - 4i$ in $\mathbb{Z}[i]$.

    (a) Use the Euclidean algorithm to compute the greatest common divisor of x and y in $\mathbb{Z}[i]$.
    (b) Find the prime factorizations of x and y in $\mathbb{Z}[i]$. Justify that your factors are indeed prime.