Math 103b Winter 2006 Final Exam review guide

Chapter 12-13

Definitions: Ring (don't need to memorize definition, just know basically what it is), identity element, commutative/noncommutative ring, unit, subring, zero-divisor, domain, field, characteristic of a ring (I only defined this for rings with identity.)

Examples: Know what the most basic examples of rings are and some of their properties. Rings of numbers ($\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, all are domains, the last three are fields, all have characteristic 0). $\mathbb{Z}_m$, the integers modulo m, for any $m \geq 2$ (a field if m is prime, not even a domain if m composite, characteristic is m). Matrix rings: $M_2(F)$, which is 2×2-matrices with entries from F. Here F could be any of the rings of numbers above, or even $\mathbb{Z}_m$ for some m (Matrix rings are the simplest examples of noncommutative rings.) Polynomial rings $R[x]$, where R is a commutative domain (studied in detail later especially when R is a field). The Gaussian integers $\mathbb{Z}[i]$, which is a special case of rings of the form $\mathbb{Z}[\sqrt{d}]$ we studied later. We also showed $\mathbb{Q}[\sqrt{2}]$ is a field at this point, which turns out to be a special case of our later work on fields.

Theorems: Basic properties of rings like $0r = 0$ for all $r \in R$. Subring test. **Cancellation property in domains (know proof).** A finite integral domain is a field (So $\mathbb{Z}_p$ for prime p is a field.) The characteristic of a domain is 0 or a prime.

Chapter 14

Definitions: Ideal, factor ring, prime ideal, maximal ideal, principal ideal generated by $a \in R$ where R is a commutative ring (written $\langle a \rangle$).

Theorems: Given any ideal I of a ring R, the factor ring R/I is a well-defined ring. If R is commutative with identity, then R/I is a domain if and only if I is a prime ideal, and R/I is a field if and only if I is a maximal ideal.

Techniques: Be able to multiply and add cosets and work with factor rings. Be able to decide if ideals are prime or maximal, based on where the factor rings are domains or fields, and vice versa.

Chapter 15

Definitions: Homomorphism and isomorphism, kernel and image of a homomorphism [*The field of quotients of a commutative domain will not be tested.*]

Theorems: Basic properties of homomorphisms. The 1st isomorphism theorem— for a homomorphism $\phi : R \to S$, $R/\ker\phi \cong \operatorname{Im}\phi$. Given any ring R with identity, there is a homomorphism $\mathbb{Z} \to R$ sending a to $a \cdot 1$—the kernel of this homomorphism is exactly $\langle m \rangle$, where m is the characteristic of R.

Techniques: Understand some important examples where factor rings can be shown to be the same as other familiar rings. Be able to use the 1st isomorphism theorem to do this in some easy examples like $\mathbb{Z}/\langle m \rangle \cong \mathbb{Z}_m$. **Understand problems about factor rings of $\mathbb{Z}[i]$ such as proving $\mathbb{Z}[i]/\langle 2-i \rangle \cong \mathbb{Z}_5$. Another example like that was on exam #2. Look over those problems again.**

Chapter 16

Definitions: Polynomial ring $R[x]$ (for any commutative ring R w/1), evaluating a polynomial at some a, division algorithm, degree of a polynomial, leading coefficient, constant, PID.

Theorems: $R[x]$ is a domain if and only if R is a domain. Division algorithm for $F[x]$ where F is a field. Remainder and factor theorems. A polynomial of degree n in $F[x]$ has at most n roots in F (counting multiplicity.) $F[x]$ is a PID.

Techniques: Be able to do the division algorithm over any field, including $\mathbb{Z}_p$. Be able to use the Remainder theorem to find the remainder when dividing by $(x-a)$, without actually using the division algorithm (several of you tripped up on this on Exam #2.) **Know how to prove that $\mathbb{R}[x]/\langle x^2+1\rangle \cong \mathbb{C}$ (in notes and book), and the similar homework problem that $\mathbb{Q}[x]/\langle x^2-2\rangle \cong \mathbb{Q}[\sqrt{2}]$.** The Chapter 16 proofs of these results use an evaluation map and the 1st homomorphism theorem. Now that we know a little field theory, you could also use the "big theorem" we stated in class on 3/8.

Chapter 17

Definitions: Reducible and irreducible polynomials in $R[x]$ (case where $R = F$ is a field most important).

Theorems: F a field. A polynomial $f \in F[x]$ of degree 2 or 3 is reducible over F if and only if it has a root in F. A polynomial in $\mathbb{Z}[x]$ which is irreducible over $\mathbb{Z}$ is also irreducible over $\mathbb{Q}$. **The mod p irreducibility test (know basic idea of proof as well as how to use).** $\langle f(x)\rangle$ is a maximal ideal of $F[x]$ if and only if $f(x)$ is an irreducible polynomial.

Techniques: Be able to decide if a polynomial $f \in F[x]$ is irreducible or not using the above theorems. Be able to use this to decide if $\langle f(x)\rangle$ is maximal and if $F[x]/\langle f(x)\rangle$ is a field.

Chapter 18

Definitions: Irreducibles, primes, and associates in any commutative domain R with 1. (The definitions of irreducibles for $F[x]$ above are just a special case.) Norm of elements in the ring $\mathbb{Z}[\sqrt{d}]$ (where d is not divisible by the square of a prime) UFDs. [*Euclidean domains will be omitted from the exam.*]

Theorems: Know the basic facts about the norm function for rings $\mathbb{Z}[\sqrt{d}]$. A PID is a UFD, so $F[x]$ and $\mathbb{Z}$ are UFDs.

Examples: Have a basic idea of which rings are UFDs and which aren't. $\mathbb{Z}, \mathbb{Z}[x], \mathbb{F}[x], \mathbb{Z}[i]$ are UFDs. The only rings we showed are not UFDs are certain rings of the form $\mathbb{Z}[\sqrt{d}]$ (you don't need to memorize for which d's.)

Techniques: be able to study irreducibles, units, associates, and be able to factor elements in rings like $\mathbb{Z}$ and $F[x]$, and most importantly, the rings $\mathbb{Z}[\sqrt{d}]$ (using properties of the norm function.) Review the last problem on exam #2, and the various homework exercises about $\mathbb{Z}[\sqrt{d}]$.

Chapter 19

Definitions: Vector space V over a field F (just understand basic idea, don't memorize definition), Basis of a vector space, Dimension of a vector space, subspace of a vector space.

I covered this section quickly and you are not expected to know anything really deep. The assigned Chapter 19 homework problems from HW #7 should give you an idea of what is expected at the very most. We only talked about vector spaces so we could use them a little in the theory of fields and the theory of error correcting codes.

Chapters 20-21

You are responsible for only very selected facts from these chapters; Most importantly, use the problems on HW #7, #8 as a guide: make sure you have a basic understanding of the problems about fields on these HW's.

Definitions: Field extension $F \subset E$. Splitting field of a polynomial $f(x) \in F[x]$ which splits in E. Minimal polynomial $g(x) \in F[x]$ of $\alpha \in E$ which is a root of some $f \in F[x]$. The notation $F(a_1, a_2, \ldots, a_n)$ for $a_i \in E$ (this is the smallest subfield of E containing F and all a_i).

Theorems: Big theorem presented in class on 3/8. If $g(x) \in F[x]$ is the minimal poly of $\alpha \in E$, then $F(\alpha) = F + F\alpha + \cdots + F\alpha^{n-1}$, where $n = \deg g$, which is an n-dimensional vector space over F. Also $F(\alpha)$ is isomorphic to $F[x]/\langle g(x) \rangle$.

Techniques: Concentrate on the case $F = \mathbb{Q} \subset E = \mathbb{C}$. Be able to write down the splitting field of a polynomial $f(x) \in \mathbb{Q}[x]$ for which you can find the roots. Be able to simplify the notation $\mathbb{Q}(a_1, \ldots, a_n)$ directly from the definition (for example, proving that $\mathbb{Q}(1, -1 + \sqrt{-3}/2, 1 - \sqrt{-3}/2)$ is really just the same as $\mathbb{Q}(\sqrt{-3})$ (HW #7). Be able to find the minimal poly

of some $\alpha \in \mathbb{C}$ (usually in problems it is not hard to find some polynomial $g(x) \in \mathbb{Q}[x]$ with α a root; then you just have to prove $g(x)$ is irreducible). Be able to identity explicitly what $\mathbb{Q}(\alpha)$ is using the big theorem and do calculations like find inverses of elements in there (see HW#8).

Chapter 31

You are responsible only for those things about codes which we covered in lecture. The single problem on error correcting codes on HW#8 is a good guide for what you should know how to do.

Definitions: Basic ideas of error correction and detection. An (n, k) binary code. $d(v, w)$. $wt(v)$. Weight of a code. Hamming code given by an $n \times k$ Matrix G. Parity check matrix H.

Theorems: Most important: A code of weight at least $2t+1$ can correct any t errors or detect any $2t$ errors. Understand the basic idea of the proof (all code words are "far apart" from each other in distance), but you won't be asked to reproduce the proof. Understand the main ingredients that go into the proof: $wt(u - v) = d(u, v)$. The triangle inequality $d(u, w) \leq d(u, v) + d(v, w)$. Theorem about how the parity check matrix can be used to correct a single error (don't need to know proof, just how to use.)

Techniques: Finding the weight of a code by writing down all of the code vectors and inspecting (or in some other way). Finding the number of errors a code can detect or correct using the main theorem. Correcting or detecting errors by checking against the list of code words. Detecting and correcting an explicit single error using the parity check matrix.

Homeworks

Look over past homeworks, but the longer "proof" problems you will not be responsible for reproducing on an exam. HW #7 and #8 are especially crucial to know because that material is fresher and has had less time to sink in, and plus it hasn't been tested yet so there will definitely be some problems like those on the exam.