Math 103b Winter 2008 Final exam review sheet

Material covered on shorter exam problems

Some topics are omitted from this list because they are covered by the essay questions below. Further questions will not be asked about these topics. The material on error-correcting codes is starred because this topic will definitely appear on the exam.

Some definitions

• Ring (but I will not ask you to check that something is or is not a ring directly from the definition).

• Identity element of a ring.

• Commutative ring.

• Unit.

• Subring.

• Zero-divisor.

• Integral Domain. (Recall this means that R is commutative with unity, and that ab = 0 implies a= 0 or b= 0.)

• Field.

• Cancelation property.

• Characteristic of a ring. (I only care about characteristic for rings R with identity, and I define it to be the smallest positive integer n such that $n \cdot 1 = 0$, or if no such n exists the characteristic is defined to be 0.)

• Ideal.

• Factor ring.

• Prime ideal.

• Maximal ideal.

• Homomorphism and isomorphism.

• Kernel and image of a homomorphism.

• Irreducible and reducible elements in a polynomial ring $R[x]$, where R is an integral domain (chapter 17)

• More generally, irreducible elements, reducible elements, and associates in any integral domain R (chapter 18)

• a principal ideal domain (PID).

** An (n, k)-linear code over $\mathbb{Z}_2$. The weight $w(v)$ of a vector v and the distance $d(u, v)$ between vectors u and v. The weight of a code. The error-correcting capability and error-detection capability of the code.

Examples of Rings

We have studied only a few classes of rings. You should know what all of these and be able to work with them.

• Rings of numbers: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

• $\mathbb{Z}_m$, the integers modulo m, for any $m \geq 2$.

• 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.

• The Gaussian integers $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$, where $i = \sqrt{-1}$. (This is a special case of the rings $\mathbb{Z}[\sqrt{d}]$ below, where $d = -1$.)

• The ring of polynomials $R[x]$, which consists of all elements of the form $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, where the coefficients a_i all come from an integral domain R.

• The ring $\mathbb{Q}[\sqrt{m}]$, where m is a positive integer which is not a square. This ring consists of all elements $\{a + b\sqrt{m} | a, b, \in \mathbb{Z}\}$. (I only did the case $m = 2$ on the board, but the same construction works for any m.)

• Given any two rings R and S, the direct sum of R and S is a new ring $R \oplus S = \{(r, s) | r \in R, s \in S\}$, with component-wise addition and multiplication.

•The rings $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} | a, b \in \mathbb{Z}\}$. We always assume that d is not divisible by the square of a prime. Then the *norm* function $N(a + b\sqrt{d}) = |a^2 - db^2|$ has lots of useful properties which you should know: (1)$N(xy) = N(x)N(y)$; (2) $N(x) = 1$ if and only if x is a unit; (3) $N(x) = 0$ if and only if $x = 0$; (4) if $N(x)$ is a prime number then x is irreducible.

Important theorems and techniques

• Know how to check if a subset of a ring is a subring.

• Know that $\mathbb{Z}_m$ is a field precisely when m is prime, and understand why $\mathbb{Z}_m$ fails to be even an integral domain when m is not prime.

• Understand the example $\mathbb{Q}[\sqrt{2}]$ and *understand the proof that it is a field.*

• Understand the theorem that the characteristic of a domain is a prime number (or 0).

• Know how to check if a subset of a ring is an ideal of the ring.

• Given a commutative ring R with element a, know the definition of the *principal ideal generated by* a, written $\langle a\rangle$.

• Understand the definition of a factor ring and how to do addition and multiplication in such a ring.

• Understand some important examples where factor rings can be shown to be the same as other familiar rings. For example:

$$\mathbb{Z}/\langle m\rangle \cong \mathbb{Z}_m. \quad \mathbb{R}[x]/\langle x\rangle \cong \mathbb{R}. \quad \mathbb{Z}[i]/\langle 2-i\rangle \cong \mathbb{Z}_5.$$

• Know the theorem that a ideal I of a commutative ring R is prime if and only if R/I is a domain, and that I is maximal if and only if R/I is a field. As a special case, know that a commutative ring R with unity is a field if and only if R and $\{0\}$ are the only ideals of R.

• Be able to check if a function between two rings is a homomorphism, and if it is a isomorphism.

• Know that the kernel of a homomorphism $\phi : R \to S$ is always an ideal of R , and the image of a homomorphism is always a subring of S. Know the statement of the 1st isomorphism theorem: $R/\ker\phi \cong \operatorname{Im}\phi$ and how to use it.

•Know what the polynomial ring $R[x]$ is, for any commutative ring R with unity.

•Know when $R[x]$ is an integral domain (this is if and only if R is an integral domain) and why this is true.

•Understand the statement of the division algorithm for the ring $F[x]$ where F is a field. Be able to state the algorithm, and perform it over various fields F (This is easy for $F = \mathbb{R}$, $\mathbb{Q}$, or $\mathbb{C}$, but takes a little more thought if $F = \mathbb{Z}_p$.)

•Understand the Remainder and Factor Theorems, and their proofs. We did the proofs in class.

•Know the definition of a PID (principal ideal domain), and the theorem that $F[x]$ (for a field F) is a PID. Understand the fact in Theorem 16.4 that any ideal I is equal to $\langle g\rangle$ where g can be any nonzero polynomial in I of minimal degree.

•Be able to prove facts like $\mathbb{R}[x]/\langle x^2+1\rangle \cong \mathbb{C}$ (Example 3 in Chap 16), using the 1st isomorphism theorem and Theorem 16.4. The method of Chap 16, Exercise 40 is similar.

•Be able to decide if a polynomial $f \in F[x]$ of degree 2 or 3 is irreducible, by checking if f has a root in F. If $F = \mathbb{Q}$ you can use the rational-root test to see if it has a root. If $F = \mathbb{Z}_p$ you check if f has a root by trial and error.

•Understand the mod p irreducibility test. This can sometimes be used to prove that polynomials in $\mathbb{Z}[x]$ of degree 4 or higher are irreducible over $\mathbb{Q}$, or gives an alternative to the rational-root test for polynomials of degree 3.

•Understand the theorem that $\langle f(x)\rangle$ is a maximal ideal of $F[x]$ if and only if $f(x)$ is irreducible. Be able to use this to decide if a (principal) ideal in $F[x]$ is maximal, and therefore to decide if $F[x]/\langle f\rangle$ is a field or not.

** Understand the main theorem on error-correcting capacity and error-detecting capacity of a code, and the idea of its proof. Be able to decide, given a code, what its error-correcting and detecting capacity are. Be able to detect and/or correct errors using a given code.

Essay questions

Be careful not to be too long-winded in these essays. The target length is about 2 pages. Also, don't overprepare. Prepare only until you are confident you understand all of the steps in the answer, then write a fresh answer on exam day. Do not attempt to memorize your answer. You may discuss these questions with classmates in the early stages as you are formulating your ideas. But if you decide to write out rough drafts as practice, these draft versions may not be shared with your classmates.

I. Discuss the theory of constructibility we developed in class in an essay. Your essay should include the following:

1. A brief outline of the basic definitions of what it means to construct points in the plane with straightedge and compass, and what constructible numbers and angles are.

2. A recalling of the main theorem we proved that characterizes which numbers are constructible in terms of chains of fields (we stated this as a theorem— in the book, it is hidden in the next to last paragraph on page 393.) Give the idea behind the proof of this theorem in a few sentences, but without details.

3. Given $\alpha \in \mathbb{R}$, briefly explain what the notations $\mathbb{Q}(\alpha)$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ mean. Explain why, if $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is not a power of 2, then α is not a

constructible number. Mention what results from the theory of field extensions you are using in your proof.

4. Show that a regular 9-gon is not constructible with straightedge and compass, given that $\alpha = \cos 20^\circ$ satisfies the relation $8\alpha^3 - 6\alpha - 1 = 0$.

II. Discuss the theory of unique factorization in an essay. Your essay should include the following:

1. The definition of a unique factorization domain (UFD).
2. A brief (couple of sentences) explanation of why the ring $F[x]$, where F is a field, is a UFD.
3. A complete proof that the ring $R = \mathbb{Z}[\sqrt{-7}]$ is not a UFD, by showing that 8 has two essentially different factorizations in this ring. Be sure to prove all of the facts you need to be sure that R does not satisfy the definition of a UFD. Use freely whatever facts about the norm you need.

III. Discuss how to construct finite fields in an essay. Your essay should include the following:

1. A proof that $\mathbb{Z}_p[x]/\langle f\rangle$, where f is irreducible of degree n, is a finite field with p^n elements. Quote the theorems that go into your argument.
2. A proof that there exists a field with exactly 16 elements. (In fact, for every prime power p^n there is always a field with exactly p^n elements, but you are only asked to do this for $p = 2$, $n = 4$.)