Math 103b Winter 2006 Exam 2 review sheet

Important definitions, theorems and techniques

0.1 Chapter 15

•Know the theorem that a commutative domain R w/1 has a field of quotients (I called it the field of fractions). Understand the basic construction of the proof, i.e. how the field of fractions is defined, but you don't need to be able to reproduce the proof.

•Know how this plays out in some easy examples. The field of fractions of $\mathbb{Z}$ is $\mathbb{Q}$. The field of fractions of $\mathbb{Z}[i]$ is $\mathbb{Q}[i]$ (this was a homework exercise). The field of fractions of $F[x]$ is just the set of formal quotients $\{f(x)/g(x)|f(x), g(x) \in F[x], g(x) \neq 0\}$ of two polynomials, with the obvious operations.

0.2 Chapter 16

•Know what the polynomial ring $R[x]$ is, for any commutative ring R w/1.

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

•Understand 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.* (The proofs are very short, but they are not in the chapter; see class notes, or the solutions in the back to Exercises 16.5 and 16.7.) Be able to use the Remainder theorem to find the remainder when dividing by $(x-a)$, without actually using the division algorithm (e.g. Exercise 16.49.)

•Know the Theorem that a polynomial of degree n in $F[x]$ has at most n roots in F (counting multiplicity.)

•Know the definition of a PID (principal ideal domain), and the theorem that $F[x]$ (for a field F) is a PID, *and its proof.*

•Understand what it means to evaluate a polynomial at some number (this just means plug in the number for x). Understand the proof that $\mathbb{R}[x]/\langle x^2+1\rangle \cong \mathbb{C}$ (in book and in notes), and the similar proof that $\mathbb{Q}[x]/\langle x^2-2\rangle \cong \mathbb{Q}[\sqrt{2}]$ (this was a homework exercise.)

0.3 Chapter 17

•Understand the definition of reducible and irreducible polynomials in $R[x]$. Understand the differences between the cases where $R=\mathbb{Z}$ or $R=F$ is a field. In $F[x]$, a polynomial f is reducible if and only if $f=gh$ where g and h have smaller degree than f. Over $\mathbb{Z}[x]$ this is not true ($2x$ is reducible since $2x=(2)(x)$ and 2 and x are both not units in $\mathbb{Z}[x]$.

•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.

•Understand how to decide if a polynomial in $f\in F[x]$ of degree 4 or 5 is irreducible, in case $F=\mathbb{Z}_p$ for some small p. Here you have to check if f has any factor of degree 1 or 2, and there are just finitely many possible factors to check. See Examples 17.7, 17.8 in the book and class notes.

•Know the theorem that a polynomial in $\mathbb{Z}[x]$ which is irreducible over $\mathbb{Z}$ is also irreducible over $\mathbb{Q}$.

•Understand the mod p irreducibility test, and be able to use it to prove that polynomials (of small degree) in $\mathbb{Z}[x]$ are irreducible over $\mathbb{Q}$. Also this can be used to prove that polynomials in $\mathbb{Q}[x]$ are irreducible, by first multiplying by something to clear the denominators. See examples in book and homework exercises. *Also, understand the proof of the mod p irreducibility test.*

•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.

•Understand how to use this to create new fields. Given any irreducible polynomial $f(x)$ in $F[x]$, $E = F[x]/\langle f(x)\rangle$ is a field. If $F = \mathbb{Z}_p$ and f has degree n, then E will be a field with p^n elements— understand the basic idea why that is true (Exercise 17.6.) Be able to create fields with p^n elements this way, for small p and n. (Say $n = 2$ or 3; then one just needs to find an irrreducible polynomial of degree n over $\mathbb{Z}_p$, which can be done by educated guessing to find a polynomial with no roots in $\mathbb{Z}_p$.)

0.4 Chapter 18

•Understand definitions of irreducibles, primes, and associates in any commutative domain R with 1. (The definitions of irreducibles for $F[x]$ above are just a special case.)

•Understand what elements are units and what elements are associates of each other in simple rings like $\mathbb{Z}$ and $F[x]$ (see class notes)

•Be able to work with the rings $\mathbb{Z}[\sqrt{d}]$. 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. *understand the proofs of facts (2-4)* (see solution to Exercise 18.1 in the back of the book, or your class notes).

•Understand the examples in class and the homework exercises about $\mathbb{Z}[\sqrt{d}]$. (In class we looked at certain elements in $\mathbb{Z}[\sqrt{-3}]$ and in $\mathbb{Z}[\sqrt{5}]$.) Understand the general techniques for working in these rings using the norm. For example, be able to show certain elements in these rings are irreducible using the methods in those examples above.

•Understand the relationship between prime and irreducible elements. Prime implies irreducible; but there are rings with elements that are irreducible but not prime (for example $\mathbb{Z}[\sqrt{-3}]$). In a PID, prime and irreducible elements are the same thing.

•Know the definition of a UFD (unique factorization domain).

•Know the theorem that a PID is a UFD (but not proof.) Understand that this means that $\mathbb{Z}$ and $F[x]$ are UFDs. Understand how to write an

element in these rings as a product of irreducibles, and what "uniqueness up to associates" means in $F[x]$.

•Know the definition of a Euclidean domain (ED). (My definition is shorter than the books definition, but either is OK.)

•Know the theorem that a ED is a PID, *and its proof.* The proof is just a small generalization of the proof that $F[x]$ is a PID, which I also asked you to know above, so you don't really need to learn two seperate proofs.

•Know that $\mathbb{Z}[i]$ is a ED, and thus a UFD. So rings of the form $\mathbb{Z}[\sqrt{d}]$ are sometimes UFDs ($d = -1$) and sometimes not ($d = -3$–showed in class, also the book shows that $d = -5$ is not a UFD. You are not expected to memorize the elements used to show these are not UFDs.)

•Understand the relationships between the various kinds of rings. ED implies PID, and PID implies UFD. But the reverse implications are not true. $\mathbb{Z}[x]$ is a UFD but not a PID. Understand thus that many of the rings we have encountered are UFD's: For example $\mathbb{Z}, F[x], \mathbb{Z}[i]$. (Also $\mathbb{Z}[x]$, by a theorem we didn't prove: If R is a UFD then $R[x]$ is a UFD.)

Homework

Review all of the homework problems on homeworks 4-6, not just the ones already mentioned above.