**List of topics for the Math 323 final exam, April 12 2014.**

The exam will be approximately 2/3 on rings, with emphasis on irreducibility of polynomials and construction of field extensions (the things that happened after the midterm) and 1/3 on modules. It covers:

(1) **Basics:** Sections 0.2, 0.3, 7.1-7.4, 7.5(only the case of integral domains), 7.6;
(2) **Euclidean rings, PIDs, UFDs:** 8.1-8.3 (though you do not need to know the proof that $\mathbb{Z}[\frac{1+\sqrt{19}}{2}]$ is not Euclidean but is a PID, which is scattered around Chapter 8).
(3) **Factorization of polynomials:** Sections 9.1-9.4.
(4) **Construction of field extensions:** 13.1 (including the construction of a field with $p^n$ elements, where $p$ is a prime).
(5) **Modules: basic definitions and examples**: Sections 10.1-10.3.
(6) **Classification of modules over PIDs:** Section 12.1.

Here is a detailed list of topics.

*I think the best way to use the list is look at the items with closed book, try to recall all the relevant definitions, facts, proofs, and examples, and if any of this is causing difficulty, then read the relevant section again. If you feel you do not understand some of these topics, also please come and get help!*

**Rings:**

(1) The definitions of a ring, commutative ring, ring with identity, homomorphism and isomorphism of rings.
(2) Key examples: the quaternions, quadratic integer rings, polynomial rings, rings of functions on a set, matrix rings.
(3) Properties of elements in rings: units, zero divisors, nilpotent elements. Examples of these types of elements in the rings listed above. Integral domains.
(4) Ideals – the definition; the notion of a quotient ring.
(5) The notion of generators of an ideal; need to know the definitions of a sum/product/intersection of ideals, inclusions between these, and be able to compute some examples. Principal ideals; examples of non-principal ideals.
(6) The four isomorphism theorems. Be prepared for questions such as "find such-and-such quotient ring", which means, identify the quotient $R/I$ for some ring $R$ and an ideal $I \subset R$ as one of the familiar examples. Also, be ready for questions such as "are these two rings isomorphic?" (similar to homework, e.g. $\mathbb{Z}[i]$ is not isomorphic to $\mathbb{Z}[\sqrt{2}]$).
(7) The notions of prime and maximal ideal. The criterion for an ideal to be prime/maximal. Why a maximal ideal is always prime. Examples of prime ideals that are not maximal.
(8) Prime and irreducible elements. Factorization into irreducibles. Examples in polynomial rings and quadratic integer rings. Be prepared for questions such as, "is such-and-such element of $\mathbb{Z}[\sqrt{-11}]$ irreducible" (or prime)?
(9) Euclidean domains, principal ideal domains, unique factorization domains; inclusions between these classes of rings. Also, need to know examples of rings that belong to one class but not the other (for example, PID but not Euclidean, etc.)

(10) Need to know some basic examples in quadratic integer rings, in particular, be able to detect (for small values of $D$ that we have discussed) if the given quadratic integer ring has unique factorization or not.
(11) The ring of polynomials over a field is Euclidean (division algorithm for polynomials).
(12) Chinese Remainder Theorem for rings, and consequences, especially for polynomial rings.
(13) Gauss' Lemma about factorization of polynomials.
(14) The theorem that $R$ is a UFD if and only if $R[x]$ is a UFD.
(15) Eisenstein's criterion of irreducibility of polynomials.
(16) Obtaining field extensions as quotients of polynomial rings (Section 13.1). You need to know how to construct a field in which a polynomial $f(x)$ that is irreducible over a given field $K$ has a root (remember, such a field can be obtained as a quotient of the polynomial ring: take $L = K[x]/(f)$. Then the class of the polynomial $x$ in this quotient ring is a root of $f$ in $L$). Need to understand how to use such quotients to construct finite fields, and be able to do computations in the resulting fields (e.g. be able to answer this type of questions: let $\alpha$ be a root of the polynomial $x^3 - x + 1$ in the field of 27 elements $\mathbb{F}_{27}$. Express the inverse of $\alpha$ as a polynomial in $\alpha$.)

Please make sure you never confuse finite fields with quotient rings of $\mathbb{Z}$: $\mathbb{F}_3$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$, but $F_{27}$ is NOT isomorphic to $Z/27\mathbb{Z}$.

Also, need to know why, for example, the rings $\mathbb{Z}[x]/(x^2+3)$ and $\mathbb{Z}[\sqrt{-3}]$ are isomorphic, but $\mathbb{Z}[x]/(x^2+3)$ and $\mathbb{Z}[x]/(x^2+1)$ are not isomorphic.

**Modules:**

(1) The definition of a module over a ring. Main examples: $\mathbb{Z}$-modules are abelian groups; $F$-modules (where $F$ is a field) are vector spaces over $F$; $F[x]$-modules are vector spaces with a linear operator.
(2) Module homomorphisms. Need to be able to compute things like $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, Z/m\mathbb{Z})$). Need to know when $(V_1, T_1)$ and $(V_2, T_2)$ are isomorphic as $F[x]$-modules.
(3) Free modules, torsion modules. Need to know and be able to use in proofs at least one definition of a free module. Need to know examples of torsion modules, and torsion-free but not free modules (and when such examples exist). The definition of a cyclic module. Examples of cyclic and non-cyclic modules.
(4) Direct sums, direct products, quotients of modules. Relevant interesting examples (is a quotient of a free module free? Is a direct sum of free modules free? Is a quotient of a torsion module always a torsion module? Is a direct sum of torsion modules torsion? What about infinite sums/products of free modules? etc.)
(5) Chinese Remainder Theorem for modules. The notion of a $p$-primary component (see Exercises to 10.3, and 12.1).
(6) The theorem that over a PID, a submodule of a free module is free (Theorem 4 in 12.1). Need to be able to use this theorem to compute things like a quotient of $\mathbb{Z}^3$ by the submodule generated by two given vectors.
(7) Structure theorem for modules over PIDs. Invariant factors and elementary divisors. Need to be able to switch between these two forms, and apply this theorem to classification of Abelian groups. Also, think about what this theorem gives for other PIDs we know about, for example, $\mathbb{Z}[i]$.