Math 5320, Topics list for the final exam

You will be allowed to bring a page of notes to the exam consisting of one piece of standard size (8.5×11) paper.

This is list of topics which may appear the final exam. It's meant to be helpful, but may not be exhaustive. To help you in your studies, I've listed some corresponding sections of the book, but keep in mind that not everything in those sections was covered in class (so you need not be concerned with it for the exam) and not everything that was covered in class is exactly in the book. So, I recommend looking back through your notes, problem sets and daily worksheets to help you study. I highly suggest making sure you're ready to give definitions of terminology in the course and making sure you understand any questions that you missed on the midterms.

The final exam will be comprehensive, but emphasize material that came after the last midterm.

The material covered by midterm I:

- Rings, subrings, fields, ring homomorphisms, integral domains, ideals and quotient rings (roughly 11.1-11.4), product rings, maximal ideals (11.8), prime ideals (the reference for these is probably the course notes. We also talked about them a lot in connection with the ch. 12 material on prime elements)
- Results related to quotients: The first isomorphism theorem and the correspondence theorem for ideals (11.4), those problems where we modded out by ideals generated by more than one polynomial (see end of 11.4)
- Product rings, Chinese remainder theorem (11.6)

The material covered by midterm II:

- Euclidean domains, the Euclidean algorithm (12.2), also (we did this separately, later) performing the division algorithm with monic divisors (see example 11.3.16 for instance)
- Principal ideal domains, finding generators of ideals in principal ideal domains, unique factorization domains, prime elements, irreducible elements. Showing that a Euclidean domain is a PID and a PID is a UFD. (12.2)

The material covered by midterm III:

- 12.3: Showing $\mathbb{Z}[x]$ is a UFD, primitive polynomials, Gauss's lemma, the relationship between irreducible polynomials of $\mathbb{Z}[x]$ and irreducible polynomials in $\mathbb{Q}[x]$.
- 12.4: More about finding irreducible polynomials. There was some discussion of modding coefficients out by a prime and using the sieve of Eratosthenes. Eisenstein's criterion. The application of Eisenstein's criterion to finding the irreducible polynomials of primitive p-th roots of unity.
- 12.5: We didn't discuss it much in lecture, but there was an extended homework assignment on the prime elements of $\mathbb{Z}[i]$.
- Start of fields (15.1-15.3): field extensions, how to adjoin an element, algebraic vs transcendental, irreducible polynomial for an element, degree of a field extension, the relationship between the degree of a primitive field extension and the degree of the irreducible polynomial of the primitive element, finding a basis for a field extension, degreees of field extensions multiply
- Using automorphisms of fields to help find irreducible polynomials (e.g., complex conjugation of $\mathbb{C}$ is an $\mathbb{R}$-automorphism). This is covered in 15.4, but honestly I found that section a little hard to read and I think there's a better discussion in 16.4.

- Using various tools to help calculate the degree of a field extension, possibly something where we've adjoined multiple elements to a field. (Section 15.3, and there were several problems we worked in class and on the problem set)

- 16.1: Symmetric functions. Understand the definition (symmetric group acting on polynomials). Statement of the symmetric functions theorem. There was also a brief discussion about how if $f(x) \in F[x]$ splits completely in a field extension K/F, then by the Symmetric Function Theorem, any symmetric function in the roots of $f(x)$ is in F (this will be useful when lecture picks up after the exam).

- 15.6: Making field extensions by modding out by irreducible polynomials. The terminology "splits completely". Proof that fields with characteristic 0 are separable (irreducible polynomials won't have repeated roots in field extensions where the split).

- 15.8: Primitive element theorem. The proof of it gives a method for producing primitive elements of finite extensions.

After the last midterm:

- Splitting fields (16.3,16.4): How to construct them (see 15.6), their definition, etc.

- Fixed fields (16.5): See especially finding irreducible polynomials of elements over fixed fields (Theorem 16.5.2) and the Fixed Field Theorem.

- Primitive roots of unity: These have come up at many different times. We've talked about their irreducible polynomials (in the prime case, see Eisenstein's criterion in 12.4) and the Galois groups $G(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. The section 16.10 is called primitive roots of unity, but it's probably not so helpful to study since it contains material that wasn't covered in the course and my lectures included material that's not in the book.

- Galois extensions (16.6). The connection with normal and separable extensions. Equivalent characterizations of Galois extensions.

- The action of the Galois group on roots of a polynomial.

- Intermediate fields (16.6, 16.7). The "main theorem". The significance of normal subgroups of the Galois group of an extension.

- Unsolvability of the quintic (16.12). I won't examine you on the specifics of this proof, but I see that topic as an application of a lot of important concepts from the course like splitting fields and our theorems about Galois extensions and intermediate fields, and these are concepts that you should be ready to apply on the exam.

- Modules (see 14.6): Definition of a module, submodule. Examples of modules, generating sets. Noetherian rings.

- Finite fields: What we covered in lecture and the study questions can be found in (15.7). I also see this topic as an application of a number of things we've learned about field extensions and Galois theory. :)