MATH 4000/6000 – Learning objectives to meet for Exam #3

The exam covers §§3.3 – 4.2 of the textbook, the material from §4.3 discussed in the 11/8 lecture (but **not** the rest of §4.3), and the material on your HW assignments.

What to be able to state

Basic definitions

You should be able to give precise descriptions of all of the following:

- homomorphism
- kernel of a homomorphism
- ideal of a (commutative) ring
- principal ideal
- the notation $\langle a \rangle$ and (more generally) $\langle a_1, \ldots, a_k \rangle$
- definition of the quotient ring R/I (including what the elements are and how the operations are defined)
- isomorphism of rings (you are also expected to remember the definition of the terms one-to-one and onto)
- direct product of rings
- the definition of the ring of Gaussian integers $\mathbf{Z}[i]$, and the definition of the norm map $N(\cdot)$ on $\mathbf{Z}[i]$ (see HW)
- earlier definitions regarding splitting of polynomials and splitting fields (see the review sheet for Exam #2)

Big theorems

Give full statements of each of the following results, making sure to indicate all necessary hypotheses. For results proved in class, describe the components and main ideas of the proof.

- rational root theorem
- Gauss's lemma about polynomial factorizations: Let $f(x) \in \mathbf{Z}[x]$ be nonconstant. If $f(x)$ factors into two polynomials in $\mathbf{Q}[x]$, it also factors into two polynomials in $\mathbf{Z}[x]$ of those same degrees. (*Statement only*)
- theorem about irreducibility mod p vs. irreducibility over $\mathbf{Q}$ (Proposition 3.4 in the book)
- Eisenstein's criterion for ireducibility
- the kernel of a homomorphism is an ideal
- statement of the division algorithm in $\mathbf{Z}[i]$ (see HW)
- In each of the rings $\mathbf{Z}$, $F[x]$, and $\mathbf{Z}[i]$, every ideal can be generated by a single element — that is, has the form $\langle a \rangle$ for some a
- Fundamental Homomorphism Theorem

- If $f(x) \in F[x]$ is irreducible, then $K = F[x]/\langle f(x)\rangle$ is a field containing F, and $f(x)$ has a root in K.
- If $f(x) \in F[x]$ is any nonconstant polynomial, there is an extension K of F in which $f(x)$ has a root.
- If $f(x) \in F[x]$ is any nonconstant polynomial, there is an extension K of F in which $f(x)$ splits.
- If $f(x) \in F[x]$ is any nonconstant polynomial, there is a splitting field for $f(x)$ over F.
- No prime $p \equiv 1 \pmod 4$ remains prime in $\mathbb{Z}[i]$
- Every prime $p \equiv 1 \pmod 4$ can be written in the form $a^2 + b^2$ for some $a, b \in \mathbf{Z}$

What to be able to do

You are expected to know how to use the methods described in class/developed on HW to solve the following problems (not comprehensive!).

- Determine all rational roots of a given polynomial $f(x) \in \mathbf{Z}[x]$
- Argue that given polynomials are irreducible over $\mathbf{Q}$
- Establish properties of quotient rings R/I by relating these back to the properties of the original ring R
- Perform computations in quotient rings R/I. (For example, multiplying two given elements of $\mathbf{Q}[x]/\langle x^3 + x\rangle$.)
- Establish isomorphisms between rings using the Fundamental Homomorphism Theorem

Extra problems

Carefully review the HW solutions. I also recommend looking at the following problems:

§3.3: 2(a,d,g), 3, 5

§4.1: 7, 8, 14, 17, 18

§4.2: 2(c), 6(a), 11(a,b), 17

§4.3: 1, 5

Here are some more problems to try.

1. Show that if F is a field and $f(x) \in F[x]$ is an irreducible polynomial of degree 2, then $f(x)$ splits over $K = F[t]/\langle f(t)\rangle$.
2. (a) Given rings R and S, which elements of the direct product $R \times S$ are units?
   (b) Let $\phi(n)$ denote the number of units in $\mathbf{Z}_n$; for example, $\phi(6) = 2$, since the units in $\mathbf{Z}_6$ are $\bar{1}$ and $\bar{5}$. Prove that if a and b are relatively prime positive integers, then
   $$\phi(ab) = \phi(a)\phi(b).$$
3. Prove that if $\phi\colon R \to S$ is a homomorphism of rings, and R is a field, then ϕ is one-to-one.

4. Suppose that F and K are fields and $\phi\colon F \to K$ is a map satisfying $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in F$. Prove that $\phi(1_F) = 1_K$; thus ϕ is a homomorphism from F to K.

5. Show that if π is prime in $\mathbf{Z}[i]$, then $\pi \mid p$ for some prime number $p \in \mathbb{Z}$.