Math 4000 – Learning objectives to meet for Exam #3

The exam will cover §4.1–§5.1 of the textbook. This may include material from §4.1 that was covered also on your last exam.

What to be able to state

Basic definitions

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

- homomorphism of rings
- kernel of a homomorphism between commutative rings
- ideal of a commutative ring
- principal ideal
- principal ideal ring, principal ideal domain
- the ideal generated by elements $a_1, \ldots, a_k$, including the notation $\langle a_1, \ldots, a_k \rangle$
- the minimal polynomial of α over F, where α belongs to a field extension of F
- definition of the quotient ring R/I
- isomorphism of rings; you must also know the definition of the terms one-to-one and onto
- direct product of rings
- the "norm map" on $\mathbf{Z}[i]$
- prime element of $\mathbf{Z}[i]$ (these are called **irreducible elements** in your text)
- basic definitions from linear algebra (vector space over a field F, span, linear independence, basis)
- the degree $[K : F]$ of a field extension K/F

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.

- the kernel of a homomorphism is an ideal
- $\mathbf{Z}$ and $F[x]$ are PIDs
- Existence of minimal polynomials: If K/F is a field extension and $\alpha \in K$ is the root of a nonzero polynomial in $F[x]$, then there is a unique monic irreducible polynomial $p(x) \in F[x]$ with $p(\alpha) = 0$; this polynomial has the property that whenever $g(\alpha) = 0$ for $g(x) \in F[x]$, we have $p(x) \mid g(x)$.

- If $\phi\colon R \to S$ is a homomorphism, then ϕ is one-to-one if and only if $\ker(\phi) = \{0\}$.
- If $\phi\colon R \to S$ is an isomorphism, then a is a unit in R if and only if $\phi(a)$ is a unit in S. Same statement for zero divisors instead of units.
- Fundamental Homomorphism Theorem
- If m and n are relatively prime positive integers, then $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$.
- If $f(x) \in F[x]$ is irreducible, then $K = F[x]/\langle f(x)\rangle$ is a field extending F, and f has a root in K.
- If $f(x) \in F[x]$ is any nonconstant polynomial, there is an extension K/F in which f splits.
- If $f(x) \in F[x]$ is any nonconstant polynomial, there is a splitting field for f over F.
- Division theorem in $\mathbf{Z}[i]$
- Euclid's lemma in $\mathbf{Z}[i]$
- Unique factorization theorem in $\mathbf{Z}[i]$
- An odd prime p in $\mathbf{Z}$ stays prime in $\mathbf{Z}[i] \iff p$ is not of the form $x^2 + y^2 \iff$ if and only if $p \equiv 3 \pmod 4$.
- If L/K and K/F are finite field extensions, then $[L : K][K : F] = [L : F]$.
- If K/F is a finite extension, say $[K : F] = n$, then every $\alpha \in K$ is the root of a nonconstant polynomial in $F[x]$. The minimal polynomial of every such α has degree dividing n.

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!).

- Establish properties of quotient rings R/I by relating these back to the properties of the original ring R
- Recognize when two rings are isomorphic by comparing properties invariant under isomorphism (e.g., number of units or number of zero divisors)
- Establish isomorphisms between rings using the Fundamental Homomorphism Theorem
- Compute with degrees of field extensions using results discussed in class

Extra problems

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

§4.1: 7, 10, 16, 17, 18, 20

§4.2: 2(c), 11(a,b), 17

§4.3: 1, 5, 8, 9, 14

§5.1: 11(a,c,f,g,i), 13, 15, 16, 18

Here are some more problems to try.

1. Prove that $\mathbf{Z}[i]$ is a PID. (Mimic the proofs from class that $\mathbf{Z}$ and $F[x]$ are PIDs.)
2. Show that if F is a field and $f(x) \in F[x]$ is an irreducible polynomial of degree 2, then f has **both roots** over $K = F[x]/\langle f(x)\rangle$.
3. (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

   $$\phi(ab) = \phi(a)\phi(b).$$
4. Prove that if $\phi\colon R \to S$ is a homomorphism of rings, and R is a field, then ϕ is injective.
5. Let $\pi = a + bi \in \mathbf{Z}[i]$, and suppose $N(\pi) = a^2 + b^2$ is a prime p in $\mathbf{Z}$.

   (a) Let $\phi\colon \mathbf{Z} \to \mathbf{Z}[i]/\langle\pi\rangle$ be defined by $\phi(a) = \bar{a}$.

   (b) Prove that ϕ is a homomorphism. Check that $\ker\phi$ contains p.

   (c) By ruling out $\ker\phi = \mathbf{Z}$, prove that $\ker\phi = \langle p\rangle$. (Why is it enough to rule out $\ker\phi = \mathbf{Z}$?)

   (d) Prove directly that ϕ is onto.

   Hint: You may want to first prove that $\gcd(a, b) = 1$.

   (e) Deduce from (a)–(d) that $\mathbf{Z}_p \cong \mathbf{Z}[i]/\langle\pi\rangle$.
6. 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 $\phi(1_F) = 1_K$.
7. Find the degrees of the extensions $\mathbf{Q}[\sqrt{2}]/\mathbf{Q}$, $\mathbf{Q}[\sqrt{2}, \sqrt[3]{2}]/\mathbf{Q}$, $\mathbf{Q}[\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}]/\mathbf{Q}$.
8. Prove that $[\mathbf{Q}[\sqrt[5]{8}] : \mathbf{Q}] = 5$.

   Hint: First prove that $[\mathbf{Q}[\sqrt[5]{2}] : \mathbf{Q}] = 5$. How is $\mathbf{Q}[\sqrt[5]{8}]$ related to $\mathbf{Q}[\sqrt[5]{2}]$?