Math 4000 – Learning objectives to meet for Exam #3

The exam will be over §4.1–§4.2 of the textbook (not including Theorem 2.7), as well as material covered 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 of rings
- kernel of a homomorphism between commutative rings
- ideal of a commutative ring
- principal ideal
- principal ideal ring
- the ideal generated by elements $a_1, \ldots, a_k$, including the notation $\langle a_1, \ldots, a_k \rangle$
- 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 definition of the ring of Gaussian integers $\mathbf{Z}[i]$, and the definition of the norm map on $N(\cdot)$ 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.

- the kernel of a homomorphism is an ideal
- statement of the division algorithm in $\mathbf{Z}[i]$ (see HW)
- $\mathbf{Z}$, $F[x]$, and $\mathbf{Z}[i]$ are principal ideal rings
- If K/F is a field extension and $\alpha \in K$ is algebraic over F, then α is the root of an irreducible polynomial $p(x) \in F[x]$; moreover, if I is the ideal of polynomials in $F[x]$ that vanish at α, then $I = \langle p(x) \rangle$.
- 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 $f(x) \in F[x]$ is irreducible, then $K = F[x]/\langle f(x)\rangle$ is a field containing 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.

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!).

- Perform basic manipulations with ideals using their definining properties.
- 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. (E.g., finding the inverse of a given in element in $\mathbf{Z}_2[x]/\langle x^3 + x + 1\rangle$.)
- 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

Extra problems

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

§4.1: 5, 8, 16, 20

§4.2: 2(c), 11(a,b), 12

Here are some more problems to try.

1. Let R be a commutative ring. If I and J are two ideals of R, define

$$I + J = \{a + b : a \in I, b \in J\}.$$

   Show that $I + J$ is an ideal of R and that $I + J$ contains both I and J.

   Follow-up: If $R = \mathbf{Z}$, $I = \langle a\rangle$, and $J = \langle b\rangle$, where a, b are positive integers, which ideal is $I + J$? e.g., what is $\langle 19\rangle + \langle 133\rangle$?

2. Suppose that m and n are relatively prime positive integers. Define a map $\phi\colon \mathbf{Z}_{mn} \to \mathbf{Z}_m \times \mathbf{Z}_n$ by

$$\phi(\bar{a}) = (\bar{a}, \bar{a}).$$

   (a) Check that ϕ is well-defined.

   (b) Prove that ϕ is a homomorphism.

   (c) Prove that $\ker(\phi) = \{\bar{0}\}$ and conclude that ϕ is injective.

   (d) By comparing the sizes of the domain and target, deduce that ϕ is surjective. Thus, ϕ is an isomorphism.

3. Show that if F is a field and $f(x) \in F[x]$ is an irreducible polynomial of degree 2, then f splits over $K = F[x]/\langle f(x) \rangle$. (From class, you already know that K contains one root of f. The point of this problem is for you to show that K contains both roots.)

4. (a) Given rings R and S, which elements of the direct product $R \times S$ are units?

   (b) Let $\varphi(n)$ denote the number of units in $\mathbf{Z}_n$; for example, $\varphi(6) = 2$, 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

$$\varphi(ab) = \varphi(a)\varphi(b).$$

5. Use the Fundamental Homomorphism Theorem to establish the following ring isomorphisms.

   (a) $\mathbf{R}[x]/\langle x^2 + 6 \rangle \cong \mathbf{C}$.

   (b) $R[x]/\langle x \rangle \cong R$ for every commutative ring R.

   (c) $\mathbf{Z}_{18}/\langle \bar{6} \rangle \cong \mathbf{Z}_6$.

   (d) $\mathbf{Q}[x]/\langle x^2 - 1 \rangle \cong \mathbf{Q} \times \mathbf{Q}$.
   Hint: Consider the homomorphism from $\mathbf{Q}[x]$ to $\mathbf{Q}\times\mathbf{Q}$ given by $f(x) \mapsto (f(1), f(-1))$.

6. Prove that if $\phi\colon R \to S$ is a homomorphism of (commutative, nonzero) rings, and R is a field, then ϕ is injective.