Math 4000 – Learning objectives to meet for Exam #2

The exam will cover §2.3–§4.1 of the textbook (excluding §2.5). This **does not** include the material on Cauchy sequences or the construction of the real numbers. The only examinable material from §4.1 is that covered by the end of the Friday, 10/23 lecture.

What to be able to state

Basic definitions

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

- construction of **C** from **R**
- complex conjugate of a complex number
- absolute value of a complex number
- polar form of a complex number
- definition of the ring $R[x]$ (starting with a commutative ring R) and allied concepts (such as the degree of a polynomial)
- definition of an irreducible polynomial in $F[x]$ (with F a field)
- the multiplicity of a root of a polynomial
- gcd of two elements of a commutative ring
- subring of a ring
- subfield, field extension, the notation K/F
- definition of $F[\alpha]$, where F is a field and α is an element of a field extension of F
- what it means to say a polynomial $f(x) \in F[x]$ splits in an extension K of F
- what it means to say a field K is a splitting field of $f(x)$ over F
- 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

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.

- theorems associated with multiplication of complex numbers in polar form, including de Moivre's theorem
- complex conjugation preserves addition and multiplication
- there are n distinct nth roots of 1 in $\mathbf{C}$, namely the numbers $1, \omega, \omega^2, \dots, \omega^{n-1}$, where $\omega = \cos(2\pi/n) + i\sin(2\pi/n)$
- a nonzero complex number has exactly n distinct nth roots
- the quadratic and cubic "formulas"
- characterization of when $R[x]$ is a domain
- the units in $R[x]$ are precisely the units of R when R is a domain; $\deg(a(x)b(x)) = \deg a(x) + \deg b(x)$ when R is a domain
- the division theorem in $R[x]$ when the leading coefficient of the divisor is a unit, and the simplified statement when R is a field
- Euclid's lemma for $F[x]$ and the unique factorization theorem for $F[x]$
- the Fundamental Theorem of Algebra
- If K/F is a field extension and $\alpha \in K$, then $F[\alpha]$ is also a field as long as α is the root of a nonzero polynomial in $F[x]$
- rational root theorem
- Gauss's lemma about polynomial factorizations
- theorem about irreducibility mod p vs. irreducibility over $\mathbf{Q}$ (Proposition 3.4 in the book)
- Eisenstein's criterion
- the kernel of a homomorphism is an ideal
- $\mathbf{Z}$ and $F[x]$ are PIDs

What to be able to compute

You are expected to know how to use the methods described in class to solve the following problems.

- Basic computations with complex numbers, in either rectangular (i.e., $a + bi$) or polar form

- Perform "long division" of polynomials with quotient and remainder; use this to perform the Euclidean algorithm, compute gcds, and express the gcd as a linear combination

- Explicitly compute (exactly) the complex roots of given quadratic or cubic polynomials

- Determine all rational roots of a given polynomial $f(x) \in \mathbf{Z}[x]$

- Prove that given polynomials are irreducible over $\mathbf{Q}$

- If α lies in a field extension of F and α is the root of a nonzero polynomial over F, then you know $F[\alpha]$ is a field. You should be able to do explicit computations in $F[\alpha]$, e.g., add and multiply elements of $F[\alpha]$ and determine inverses for nonzero elements of $F[\alpha]$.

- Compute minimal polynomials in simple cases (see the examples discussed in class)

Extra problems

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

§2.3: 2, 7, 21, 22

§2.4: 6(a)

§3.1: 1, 2(b,c,d,e), 5, 9(c), 10(b,d,f), 11, 12, 13, 14

§3.2: 3(a,b,f)

Here are some more problems to try.

1. Let R be a domain. Show that if $a, b \in R$, then $\langle a \rangle \subset \langle b \rangle$ if and only if $b \mid a$.

2. Prove that $\mathbf{Z}[i]$ is a PID. (Mimic the proofs in class that $\mathbf{Z}$ and $F[x]$ are PIDs.)

3. (a) Find **all** of the divisors of x in the ring $\mathbf{Z}[x]$. Justify your answer.

   (b) Let I be the ideal $\langle 2, x \rangle$ of $\mathbf{Z}[x]$. Show that there is no single $f(x) \in \mathbf{Z}[x]$ with $I = \langle f(x) \rangle$. (This proves that $\mathbf{Z}[x]$ is not a PID.)

4. 4.1.3

5. 4.1.5

6. 4.1.8

7. 4.1.16

8. Let m be any integer. Prove that every ideal of $\mathbf{Z}_m$ is principal.

9. 4.1.4 (this should be easy if you have already done the above!)