MATH 4000/6000 – Learning objectives to meet for Exam #2

The exam will cover §3.1, §3.3, and §4.1, through what is covered by end of class on Monday, 3/31.

What to be able to state

Basic definitions

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

- the ring $R[x]$ (starting with a commutative ring R, not the zero ring) and allied concepts, such as the degree of a polynomial
- irreducible polynomial in $F[x]$ (with F a field)
- gcd of two elements of $F[x]$
- subring of a ring
- homomorphism
- kernel of a homomorphism
- ideal of a commutative ring
- principal ideal
- notation: xR, $\langle x \rangle$ and (more generally) $\langle x_1, \ldots, x_n \rangle$
- definition of the quotient ring R/I (including what the elements are and how the operations are defined)

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.

- If R is a domain, then $R[x]$ is a domain, and $\deg(a(x)b(x)) = \deg a(x) + \deg b(x)$ for all nonzero $a(x), b(x) \in R[x]$.
- division algorithm in $F[x]$, where F is a field
- Root-Factor Theorem and the Remainder Theorem
- If $f(x) \in F[x]$ has degree ≥ 2, and $f(x)$ has a root in F, then $f(x)$ is not irreducible.
- If $f(x) \in F[x]$ has degree 2 or 3, and $f(x)$ has no root in F, then $f(x)$ is irreducible.
- If $a(x), b(x) \in F[x]$ and $d(x)$ is a gcd of $a(x)$ and $b(x)$, then $d(x) = a(x)X(x)+b(x)Y(x)$ for some $X(x), Y(x) \in F[x]$.
- Euclid's lemma for $F[x]$ and the unique factorization theorem for $F[x]$

- Rational root theorem
- Gauss's lemma about polynomial factorizations: Let $f(x)$ be a polynomial with integer coefficients. Whenever $f(x)$ factors into two nonzero polynomials in $\mathbf{Q}[x]$, it also factors into two polynomials in $\mathbf{Z}[x]$ of those same degrees. (Statement only!)
- irreducibility mod p implies irreducibility over $\mathbf{Q}$ (HW #5, Problem 3)
- Eisenstein's irreducibility criterion
- the kernel of a homomorphism is an ideal
- every ideal of $\mathbf{Z}$ is principal
- every ideal of $F[x]$ (with F a field) is principal
- If $\phi\colon R \to S$ is a homomorphism, then ϕ is one-to-one if and only if $\ker(\phi) = \langle 0 \rangle$.
- If $f(x) \in F[x]$ has degree $n \geq 1$, then $F[x]/\langle f(x) \rangle = \{\overline{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}} : \text{all } a_i \in F\}$. Moreover, each element of $F[x]/\langle f(x) \rangle$ has a unique expression as $\overline{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}}$.

What to be able to compute

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

- Perform "long division" of polynomials with quotient and remainder; use this to carry out the Euclidean algorithm, compute gcds, and express your gcd as a linear combination of the starting polynomials
- Determine all rational roots of a given polynomial with integer coefficients
- Argue that given polynomials are irreducible over prescribed fields
- Perform computations in $F[x]/\langle m(x) \rangle$, such as addition, multiplication, and taking powers (to the extent covered by Monday, 3/31)

As usual, there will be five problems on the exam. You can expect at least one of these to ask you to decide irreducibility of given polynomials over specified fields (as in sample Problem #1). You can also expect at least one problem asking you to reason with either the definition of homomorphism (possibly also the kernel of a homomorphism) and/or the definition of an ideal; an example is Problem #4 below.

Practice problems

1. Decide whether each of the following polynomials is irreducible over the given field F. Justify your answers.
   (a) $x^3 + x^2 + 1$, $F = \mathbf{Z}_3$
   (b) $5x^3 - 2x^2 + 5x - 2$, $F = \mathbf{Q}$
   (c) $x^4 - 60$, $F = \mathbf{Q}$
   (d) $9001x^3 - 10x + 1$, $F = \mathbf{Q}$

2. (a) State Fermat's Little Theorem (yes, the result from Chapter 1!).
   (b) The number 127 is prime (you may assume this). Write down a factorization of $x^{127} - x$ into irreducibles of $\mathbf{Z}_{127}[x]$. Explain how you know all the factors appearing in your answer are irreducible.

3. For this problem, F and K are fields with F a subring of K. Let $f(x), g(x) \in F[x]$.
   (a) What does it mean to say $d(x) \in F[x]$ is a greatest common divisor in $F[x]$ of $f(x)$ and $g(x)$?
   (b) Suppose $d(x) \in F[x]$ is a greatest common divisor in $F[x]$ of $f(x)$ and $g(x)$. Since F is a subring of K, both $f(x), g(x)$ also belong to $K[x]$. Show that $d(x)$ is also a greatest common divisor in $K[x]$ of $f(x)$ and $g(x)$.

4. Let R be a commutative ring.
   (a) What does it mean to say that a subset I of R is an ideal of R?
   (b) If I and J are ideals of R, prove that $I \cap J$ is also an ideal of R.
   (c) Suppose now that $R = \mathbf{Z}$. If $I = \langle 6 \rangle$ and $J = \langle 10 \rangle$, which ideal of $\mathbf{Z}$ is $I \cap J$? Express your answer in the form $\langle n \rangle$ for a positive integer n. **No justification required.**

5. (a) What is the definition of R/I? State both the definition of R/I as a set as well as the imposed notions of addition and multiplication.
   (b) Let R be a commutative irng. Let I be an ideal of R. Suppose that I is a proper subset of R *and* that I has the following property:

   $$\text{whenever } a, b \in R \text{ satisfy } ab \in I, \text{ either } a \in I \text{ or } b \in I.$$

   Prove that R/I is an integral domain. (Your first step should be to show that R/I is not the zero ring.)

6. Let $F = \mathbf{Z}_2$.
   (a) Explain why $m(x) = x^3 + x^2 - 1$ is irreducible in $F[x]$.
   (b) List the distinct powers of $\alpha = \bar{x}$ in $\mathbf{Z}_2[x]/\langle m(x) \rangle$: $\alpha^1 = \alpha$, $\alpha^2 = \ldots$, $\alpha^3 = \ldots$, etc. Here each $\ldots$ should be an expression of the form $a_0 + a_1\alpha + a_2\alpha^2$ for some $a_0, a_1, a_2 \in \mathbf{Z}_2$.
   "Distinct" means you should stop once you know that proceeding further will never produce a power of α not already on your list.
   How many distinct powers are there?

(c) Using your answer to part (b), determine the inverse of $\alpha + 1$ in $F[x]/\langle m(x)\rangle$. Again, your answer should be an expression of the form $a_0 + a_1\alpha + a_2\alpha^2$ for some $a_0, a_1, a_2 \in \mathbf{Z}_2$.