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

The exam will cover §3.1–§3.3, through the end of class on Monday, 3/22. The material on constructing $\mathbf{R}$ from $\mathbf{Q}$ is not examinable.

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) 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, subfield of a field, field extension
- $F[\alpha]$, where F is a field and α is an element of a field extension of F
- $\alpha \in K$ is algebraic over F
- $F[\alpha, \beta]$ and more generally $F[\alpha_1, \alpha_2, \ldots \alpha_n]$

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 $F[x]$ (with F a field)
- root factor theorem and the remainder theorem
- If $f(x) \in F[x]$ has degree 2 or 3, then $f(x)$ is irreducible in $F[x] \iff f(x)$ has no roots in F.
- 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 $F[x]$
- If F is a subfield of K, and $\alpha \in K$ is algebraic over F, then $F[\alpha]$ is a subfield of K.
- If F is a subfield of K, and $\alpha \in K$ is algebraic over F, then α is the root of an irreducible polynomial $p(x) \in F[x]$.
- If F is a subfield of K, and $\alpha \in K$ is a root of an irreducible polynomial $p(x) \in F[x]$ of degree n, then $F[\alpha] = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_0, \ldots, a_{n-1} \in F\}$. Moreover, each element of $F[\alpha]$ has a unique representation in the form $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$.

- Rational root theorem
- Gauss's lemma about polynomial factorizations: Let $f(x) \in \mathbf{Z}[x]$. If $f(x)$ factors into two nonconstant polynomials in $\mathbf{Q}[x]$, it also factors into two nonconstant polynomials in $\mathbf{Z}[x]$ of those same degrees. (Statement only!)
- irreducibility mod p implies irreducibility over $\mathbf{Q}$
- Eisenstein's irreducibility criterion

What to be able to do

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
- Perform computations in $F[\alpha]$, such as addition, multiplication, and taking inverses
- Determine all rational roots of a given polynomial with integer coefficients
- Argue that given polynomials are irreducible over prescribed fields

You can expect at least one problem requiring explicit calculations in $F[\alpha]$ (compare with Problem #2 below) and at least one problem asking you to decide irreducibility of given polynomials over specified fields (as in Problem #1).

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) x^4+x+1, $F = \mathbf{Z}_2$; you may assume as known that x^2+x+1 is the only irreducible polynomial of degree 2 in $\mathbf{Z}_2[x]$

   (c) $5x^3 - 2x^2 + 5x - 2$, $F = \mathbf{Q}$

   (d) $x^4 - 60$, $F = \mathbf{Q}$

   (e) $9001x^3 - 10x + 1$, $F = \mathbf{Q}$

2. Let p be a prime number and let $F = \mathbf{Z}_p$. What are the roots of $x^p - x$ in $\mathbf{Z}_p$? How does $f(x)$ factor into irreducibles polynomials in $\mathbf{Z}_p[x]$?

   Hint. Recall the statement of Fermat's little theorem.

3. Let F be a subfield of K and let $\alpha \in K$.

   (a) What does it mean to say that $\alpha \in K$ is algebraic over F?

   (b) Let $\alpha \in K$ be algebraic over F. As discussed in class, there is an irreducible polynomial $p(x) \in F[x]$ for which $p(\alpha) = 0$. Show that if $m(x)$ is any polynomial in $F[x]$ with $m(\alpha) = 0$, then $p(x)$ divides $m(x)$ in $F[x]$.

4. Let F be a field. 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 of $f(x), g(x)$ in $F[x]$?

   (b) Suppose $d(x) \in F[x]$ is a greatest common divisor of the nonzero polynomials $f(x), g(x) \in F[x]$.
   Let $D(x) \in F[x]$ be a common divisor of $f(x), g(x)$ with largest possible degree (largest among all common divisors of $f(x), g(x)$). Prove that $D(x) = c \cdot d(x)$ for some $c \in F$.

5. A field F is called algebraically closed if for every nonconstant $f(x) \in F[x]$ there is an $\alpha \in F$ with $f(\alpha) = 0$. For example, the complex numbers (to be discussed later in the course) are an example of an algebraically closed field. This last fact is called the Fundamental Theorem of Algebra, although it is most naturally proved in courses on complex variables.

   (a) Prove that if F is an algebraically closed field, then every nonzero $f(x) \in F[x]$ has a factorization in $F[x]$ of the form

   $$f(x) = c(x - \alpha_1) \cdots (x - \alpha_n),$$

   where c is a nonzero element of F and $\alpha_1, \ldots, \alpha_n \in F$.

   (b) Suppose F is algebraically closed and that $f(x) \in F[x]$ is a nonconstant polynomial with leading coefficient 1. Write $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Show that when $f(x)$ is factored as in part (a), we have $a_0 = (-1)^n \alpha_1 \cdots \alpha_n$.

6. Let $F = \mathbf{Z}_3$.

   (a) Show that $f(x) = x^3 - x - 1$ is irreducible in $F[x]$.

   (b) **Assume** for this problem that there is that there is a field extension K of F containing a root of f. That is, F is a subfield of K and there is an $\alpha \in K$ with $f(\alpha) = 0$. State a general theorem guaranteeing that every element of $F[\alpha]$ has the form $c_0 + c_1\alpha + c_2\alpha^2$ for some $c_0, c_1, c_2 \in \mathbf{Z}_3$ and that this expression is unique.

   (c) Write α^3 in the form given in part (b).

   (d) Write $(\alpha - 1)^{-1}$ in the form given in (b).