KEY IDEAS FROM CHAPTER 9 AND SUPPLEMENTARY MATERIAL

(1) This chapter is an introduction to rings of polynomials over fields and some of their properties that are similar to properties of \( \mathbb{Z} \) that we’ve explored earlier in the course.

(2) The first key point (and one that the book doesn’t make explicit) is that, for a field \( K \), \( K[x] \) is a certain ring that contains \( K \). So we’ve got a set of “numbers”, operations of addition and multiplication that satisfy some axioms (see the key ideas handout for Chapter 6), etc. These polynomials do determine functions from \( K \) to \( K \), but that’s not what they are. In fact, as we saw concretely with \( \mathbb{F}_3[\!\times\!] \), there may be only finitely many such functions, but \( K[x] \) is always infinite because polynomials of different degrees must be distinct. (Recall that for finite \( n \), \( \mathbb{F}_n \) is our notation for the (unique up to isomorphism) field of order \( n \); it turns out that \( n \) must be a prime power. The field \( \mathbb{F}_3 \) is just \( \mathbb{Z}_3 \), but \( \mathbb{F}_9 \) is not the same as \( \mathbb{Z}_9 \), since \( \mathbb{Z}_9 \) has zero divisors.)

(3) If \( K[x] \) is a ring, then \( x \) is some element of that ring. We saw that we need \( x \) to be transcendental over \( K \), meaning that no polynomial with a nonzero coefficient is equal to the 0 polynomial. (Equivalently, no nontrivial \( K \)-linear combination of powers of \( x \) is 0, where “nontrivial” means that not all the coefficients are 0, just as in linear algebra.) We saw that, for \( K = \mathbb{F}_3 \), the nonzero polynomial \( x^3 - x \) determines a function \( \mathbb{F}_3 \to \mathbb{F}_3 \) that maps everything to 0. So as a function, \( x^3 - x \) is the constant function 0, but as a polynomial, it’s not 0.

(4) The construction of \( K[x] \) as the collection of infinite sequences of elements of \( K \) with finite support (see the handout) is one way to get our hands on a concrete element \( x \) that we can be sure is transcendental over \( K \). This construction thus gives us a way to be sure that our standard ways of writing polynomials and carrying out the operations with them really make sense.

(5) Once we prove that a polynomial of degree \( n \) determines a function \( K \to K \) that maps at most \( n \) values in \( K \) to 0 (which is what we mean when we say, somewhat sloppily, that the polynomial “has” at most \( n \) roots in \( K \)), we can see that when \( K \) is infinite, two polynomials that determine the same function \( K \to K \) must be the same as polynomials, not just functions. But this depends on the field being infinite, and it’s important to keep the notions of polynomial and polynomial function distinct, even if we find it convenient (or at least easy) to use the single term “polynomial” for both of them.

(6) It is interesting to think about much of how we work with polynomials in school mathematics. On the one hand, we’re primarily interested in using them as functions (modeling growth, solving equations, etc.), but most

Date: October 7, 2019.
of what we can do to analyze these functions really involves working in the polynomial ring. The reason is that it’s very hard to characterize the polynomial functions among the continuous functions. Suppose I give you a polynomial function \( R \to R \) of degree 8 I ask you whether it has fewer than 8 roots. Without knowing about the theory of polynomial rings, you could try looking at the intervals where the derivative is positive and negative, and trying to find the intervals where the function is positive and negative. But that’s a lot of work, and may depend on some very hard calculations (which you would probably have to approximate on a computer—if the derivative is really a polynomial function of degree 7, how do you find its zeros?). But our “abstract” analysis in the polynomial ring shows us that a polynomial of degree 8 gives a polynomial function with at most 8 roots. Even things like the quadratic formula, results about factoring, etc., are really calculations/theorems about the polynomial ring.

(7) Lots of notions that we saw first for \( Z \), like irreducibility (the K-12 notion of “prime”), the division theorem, the Euclidean algorithm for gcds, etc., make sense in \( K[x] \). (Though we won’t look at the Euclidean algorithm for a little while.)

(8) The division theorem in \( K[x] \) is one of the key tools we use, both for understanding \( K[x] \) on its own and for working out the connection between polynomials and the polynomial functions they determine. In general (as we’ll see later in the course), we want to think of the division theorem (which holds in certain classes of rings) as saying that, given two nonzero elements of the ring \( a \) and \( b \), we can write \( b \) as a multiple of \( a \) plus a remainder that is smaller in some appropriate sense, than \( a \). For the integers, “smaller” means that the remainder is strictly less than \(|a|\). For polynomials over a field, it means that the degree of the remainder is smaller than the degree of \( a \).

(9) Section 9.4 illustrates the way that we prove theorems in \( K[x] \) to get results about polynomial functions. The theorems related to the roots \( \gamma_i \) of a polynomial function \( f(x) \) and the divisibility of \( f(x) \) by the \( x - \gamma_i \) in \( K[x] \) make the key connections between polynomial functions and the polynomial ring for us. We prove these using the division theorem and related ideas. And then we can draw conclusions about the number of roots of a polynomial of degree \( n \), etc.

(10) A central idea in this part of abstract algebra is the way that the structure of a polynomial depends on what we allow for the coefficient ring. As we noted in class, polynomial \( x^2 + 1 \) could be in \( K[x] \) for any \( K \). But if \( K = Q \) or \( K = R \), the function it defines has no roots and is irreducible. If \( K = C \), however (or the much smaller field \( Q(i) \) that we’ll talk about in a while), this polynomial factors nontrivially as \((x + i)(x - i)\), and has two roots. So the behavior of a polynomial depends on the coefficient field we’re considering. In particular, we can start with, say, \( f(x) \in Q[x] \), and enlarge the field \( Q \) to make sure we get some roots of \( f(x) \). Studying how this works is the key to understanding why, for example, there are formulas for the roots of quadratic, cubic, and quartic polynomials over \( Q \), but no such formula can exist for the polynomials of higher degrees. (And also the basis for understanding why some classic geometric challenges like squaring the
circle and trisecting the angle are impossible.) The last section of Chapter 9 begins to look at these issues by considering what happens when we have two fields, $K$ and $L$, with $K \subseteq L$. (A pair of fields like this is called a field extension, though we sometimes say something like “$L$ is an extension of $K$”.)