DRAFT

Commentary Portfolio

Student #1091

February 18, 2018

Contents

Note to the reader

Given that I am struggling to find a way to turn this document into something that is useful for my future self (which would be in keeping with the stated intention for this assignment), please do not judge harshley the poor quality of the work herein. Since we are writing the commentary for our future selves, any use of the word 'you' is directed towards a future version of me, not the disinterested reader who is only reading this because they are required to do so. To belabor this point as much as possible, if I say 'you did something stupid when first learning this material,' I am calling myself stupid, something that is oft warranted.

Questions about the validity of the converse of various theorems will likely be delayed until the penultimate draft, or omitted entirely.

7 Polynomials over a Ring

7.1 Polynomials over a Ring

Commentary Section 7.1 defines polynomials, polynomial rings, the operations of polynomial addition and multiplication, and proves that these operations form a polynomial ring $A[x]$ given a ring of coefficients A. Section 7.2 demonstrates some interesting properties about polynomial rings, such as the additivity of degree in an integral domain. This section also contains useful tools such as the Division Algorithm for Polynomials, and the function $\bar{f}$. In Section 7.3 we learn to evaluate polynomials, which inherently brings along the definition of a polynomial root.

Definition 1. *Let A be a commutative ring with unity. For each nonnegative integer n and elements $a_0, a_1, \ldots, a_n \in A$ we can define a polynomial over A, $a(x)$, by:*

$$a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \qquad \text{or} \qquad \sum_{i=0}^{n} a_ix^i.$$

The set of all polynomials over a ring A is denoted $A[x]$.

Definition 4. *Suppose A is a commutative ring with unity and $a(x) \in A[x]$ with $a(x) = a_0 + a_1x + \cdots + a_nx^n$ for some nonnegative integer n.*

(i) The elements $a_0, a_1, \ldots, a_n \in A$ are the coefficients of $a(x)$.

(ii) For each $0 \leq i \leq n$, a_ix^i is called a term of $a(x)$.

(iii) The largest nonnegative integer n with $a_n \neq 0_A$ (if one exists) is the degree of $a(x)$, denoted $\deg(a(x)) = n$. So for $k > n$ we know $a_k = 0_A$.

(iv) If all coefficients of $a(x)$ are 0_A we say the degree of $a(x)$ is $-\infty$.

(v) For $n \geq 0$ if $\deg(a(x)) = n$ then a_n is called the leading coefficient of $a(x)$.

Definition 5. *Let A be a commutative ring with unity. For polynomials $a(x), b(x) \in A[x]$ we say $a(x) = b(x)$ if and only if they have the same degree and if the degree is equal to $n \geq 0$ then for every $i \leq n$, $a_i = b_i$.*

Definition 6. *Let A be a commutative ring with unity and let $a(x), b(x) \in A[x]$ as shown below.*

$$a(x) = \sum_{i=0}^{n} a_i x^i \qquad\qquad b(x) = \sum_{i=0}^{m} b_i x^i$$

We define the new polynomial $c(x) = a(x) + b(x)$ as follows where $k = \max\{n, m\}$.

$$c(x) = \sum_{i=0}^{k} c_i x^i \quad \text{and} \quad c_i = a_i + b_i$$

Remember, if $i > n$ or $i > m$ we assume $a = 0_A$ or $b = 0_A$, respectively.

Definition 8. *Let A be a commutative ring with unity and polynomials $a(x), b(x) \in A[x]$ as shown below.*

$$a(x) = \sum_{i=0}^{n} a_i x^i \qquad\qquad b(x) = \sum_{i=0}^{m} b_i x^i$$

Define the new polynomial $d(x) = a(x)b(x)$ as follows.

$$d(x) = \sum_{i=0}^{n+m} d_i x^i \quad \text{where} \quad d_i = \sum_{j+t=i} a_j \cdot_A b_t$$

Note: $0 \leq j \leq n$ and $0 \leq t \leq m$.

Commentary For arbitrary reasons I prefer to write the product of polynomials as

$$a(x)b(x) = \sum_{i+j=0}^{n+m} a_i b_j x^{i+j}.$$

Theorem 11. *Let A be a commutative ring with unity. The operations of polynomial addition and polynomial multiplication from Definitions 7.6 and 7.8 are associative in $A[x]$.*

Proof Sketch. Let $a(x), b(x), c(x) \in A[x]$, and use the definitions to show associativity. □

Theorem 13. *Let A be a commutative ring with unity. In $A[x]$, polynomial addition and polynomial multiplication are both commutative.*

Proof Sketch. Chase the definitions. □

Theorem 14. *Let A be a commutative ring with unity. Then the distributive laws hold in $A[x].$*

Proof. Let A be a commutative ring with unity. Consider the three polynomials in $A[x]$ below.

$$a(x) = \sum_{i=0}^{n} a_i x^i \quad b(x) = \sum_{i=0}^{n} b_i x^i \quad c(x) = \sum_{i=0}^{n} c_i x^i$$

Since by Theorem 7.13 polynomial multiplication is commutative we only need to show that $a(x)[b(x) + c(x)] = a(x)b(x) + a(x)c(x)$. For help with notation we will used$(x) = b(x)+c(x)$ and $a(x)d(x) = p(x)$. Thus $d_t = b_t +_A e_t$ for each $0 \leq t \leq n$. Remember that the coefficients are all from A and the distributive law holds in A, so for each $0 \leq i \leq 2n$ we can calculate p_i as seen below.

$$p_i = \sum_{j+t=i} (a_j \cdot_A d_t) = \sum_{j+t=i} (a_j \cdot_A [b_t +_A c_t]) = \sum_{j+t=i} (a_j \cdot_A b_t) +_A (a_j \cdot_A c_t)$$

If we call $s(x) = a(x)b(x)$ and $u(x) = a(x)e(x)$ then for $0 \leq i \leq 2n$ we have:

$$s_i = \sum_{j+t=i} (a_j \cdot_A b_t) \quad u_i = \sum_{j+t=i} (a_j \cdot_A c_t)$$

Clearly (as these sums are finite), $p_i = s_i +_A u_i$ for each i and so $p(x) = s(x) + u(x)$. Thus we have $a(x)[b(x) + c(x)] = a(x)b(x) + a(x)c(x)$ and the distributive laws hold. □

Theorem 15. *Let A be a commutative ring with unity. Then the set $A[x]$ of polynomials over A is a commutative ring with unity.*

Proof Sketch. Given the preceding theorems, the only missing pieces to this proof is to show that $0(x)$ and $1(x)$ are the zero and unity of $A[x]$, respectively, and that additive inverses exist. This is another case of chasing definitions, which is to say a useful exercise, but not a good use of our time here. □

7.2 Properties of Polynomial Rings

Theorem 17. *If A is an integral domain then $A[x]$ is also an integral domain.*

Proof Sketch. From Theorem 7.15 we have that A being an integral domain implies $A[x]$ is a commutative ring with unity, thus it will suffice to show that there are no zero divisors in $A[x]$, this is achieved easily with a proof by contradiction.

This theorem is pretty useful, given that fields are also integral domains. Moreover, polynomials are nicer to deal with in integral domains because degree is additive when there are no zero divisors. □

Theorem 20. *Let A be an integral domain, and nonzero $a(x), b(x) \in A[x]$. If $\deg(a(x)) = n$ and $\deg(b(x)) = m$, then $\deg(a(x)b(x)) = n + m$.*

Proof Sketch. This can be shown by easily by invoking the definitions of polynomial multiplication and zero divisors. Given that this is pretty much a direct consequence of the previous Theorem and basic definitions, I would classify this result as a corollary rather than a full fledged theorem. □

Theorem 22. *If A is a commutative ring with unity then $char(A) = char(A[x])$.*

Commentary. Given that I have yet to use this theorem as of this writing, we omit its proof. □

Theorem 24 (The Division Algorithm)**.** *Let K be a field and $a(x), b(x) \in K[x]$. If $b(x) \neq 0(x)$ then there exist unique polynomials $q(x), r(x) \in K[x]$, for which $a(x) = b(x)q(x) + r(x)$ and either $\deg(r(x)) < \deg(b(x))$ or $r(x) = 0(x)$.*

Commentary We omit the full proof here, due to the "computational tool" nature of the theorem. To my future self: If things have gone according to plan and you're a high school mathematics teacher, you do not need to jog your memory with examples of polynomial long division. If you do, you have failed.

Theorem 26. *Let K be a field. Then every ideal of $K[x]$ is a principal ideal.*

Proof. Let K be a field, and suppose S is an ideal of $K[x]$. As in the proof of Theorem 5.18, if $S = \{0(x)\}$ or $S = K[x]$, then $S = \langle 0(x)\rangle$ or $S = \langle 1(x)\rangle$, respectively, and S is principal. Thus assume that S is not one of these trivial ideals and so there is polynomial $a(x) \in S$ with $a(x) \neq 0(x)$.

As $a(x) \neq 0(x)$ then $\deg(a(x)) \geq 0$, so first assume $\deg(a(x)) = 0$. Thus $a(x)$ is a nonzero constant polynomial, $a(x) = a_0$ with $a_0 = 0_K$. We know a_0 is a unit with inverse $a_0^{-1} \in K$, and so the polynomial $b(x) = (a_0)^{-1}$ is in $K[x]$. But S absorbs products from $K[x]$ so $a(x)b(x) \in S$, or $1(x) \in S$. This contradicts that S is not equal to $K[x]$ by Theorem 5.12 and so S cannot contain a polynomial of degree 0.

Now S contains a nonzero polynomial, $a(x)$, but cannot contain a polynomial of degree 0. Thus for every nonzero $a(x) \in S$, $\deg(a(x))$ is a positive integer.

$$\text{Define B} = \{n \in \mathbb{Z} : \deg(q(x)) = n \text{ for some nonzero } q(x) \in S\}.$$

Clearly, $B \subseteq \mathbb{Z}^+$, but $\mathbb{Z}$ is an integral system (Definition 6.32) which tells us that B has a least element, call it m. By definition of B there exists some polynomial $p(x) \in S$ with $\deg(p(x)) = m$. We will now show that $S = \langle p(x)\rangle$.

As $p(x) \in S$ and S is an ideal it is clear that $\langle p(x)\rangle = S$, so we only need to show that $\langle p(x)\rangle \supseteq S$. Let $b(x) \in S$. If $b(x) = 0(x)$ then $b(x) = 0(x)p(x)$ and $b(x) \in \langle p(x)\rangle$, so assume instead that $b(x) \neq 0(x)$.

Now we know $\deg(b(x)) \in B$, which tells us that either $\deg(b(x)) = m$ or $\deg(b(x)) > m$. Using Theorem 7.24 we find polynomials $q(x), r(x) \in K[x]$ with $b(x) = p(x)q(x) + r(x)$ and $0 < \deg(r(x)) < \deg(p(x))$ or $r(x) = 0(x)$. But $r(x) = b(x) - p(x)q(x)$ and $b(x), p(x) \in S$, so as S is an ideal $r(x) \in S$. If $r(x) \neq 0(x)$ we would have a contradiction since m is the least element of B. Thus we must have $r(x) = 0(x)$ and so $b(x) = p(x)q(x)$. Hence $b(x) \in \langle p(x)\rangle$, $S = \langle p(x)\rangle$, and S is a principal ideal. □

Theorem 27. *Let A be a commutative ring with unity. Then the function $f : A \to A[x]$ defined by $f(a) = a + 0_A x$ is an injective ring homomorphism.*

Proof. Let A be a commutative ring with unity, and define $f : A \to A[x]$ by $f(a) = a + 0_A x$. To see that f is a ring homomorphism, let $a, b \in A$.

$$f(a +_A b) = (a +_A b) + 0_A x$$

$$f(a) + f(b) = (a + 0_A x) + (b + 0_A x) = (a +_A b) + 0_A x$$

Thus $f(a +_A b) = f(a) + f(b)$. Verification of $f(ab) = f(a)f(b)$ using polynomial multiplication is an exercise at the end of the chapter.

Proof of multiplicativity Let a, b be as above, and let $c = a \cdot_A b$, obviously $c \in A$.

$$f(a \cdot_A b) = f(c) = c + 0_A x$$

$$f(a) \cdot_A f(b) = (a + 0_A x) \cdot_A (b + 0_A x) = c + 0_A x$$

Thus $f(a \cdot_A b) = f(a) \cdot f(b)$.

Thus the function f is a ring homomorphism.

To see that f is injective, suppose we have $c \in A$ with $c \in \ker(f)$. Thus $f(c) = 0(x)$ since $0_{A[x]} = 0(x)$, and so $c + 0_A x = 0(x)$. This can only be true if $c = 0_A$ so $\ker(f) = \{0_A\}$. Hence f is injective by Theorem 5.29. □

Theorem 28. *Let A and K be commutative rings with unity, and suppose that $f : A \to K$ is a ring homomorphism. Then the function $\bar{f} : A[x] \to K[x]$ defined below is also a ring homomorphism.*

$$\bar{f}(a_0 + a_1 x + \cdots + a_n x^n) = f(a_0) + f(a_1)x + \cdots + f(a_n)x^n$$

Proof. Suppose A and K are commutative rings with unity, and $f : A \to K$ is a ring homomorphism. Clearly, $f : A[x] \to K[x]$ is well defined since f is well defined, and so each coefficient of $\bar{f}(a(x))$ is unique. To see that $\bar{f}$ is a homomorphism, for $a(x), b(x) \in A[x]$ we need to show that $\bar{f}(a(x) + b(x)) = \bar{f}(a(x)) + \bar{f}(b(x))$ and $\bar{f}(a(x)b(x)) = \bar{f}(a(x))\bar{f}(b(x))$. As an exercise at the end of the chapter you will show the first of these, so we will look at the second.

Suppose $a(x), b(x) \in A[x]$ and $d(x) = a(x)b(x)$.

$$a(x) = \sum_{i=0}^{n} a_i x^i \quad b(x) = \sum_{i=0}^{m} b_i x^i$$

$$d(x) = \sum_{i=0}^{n+m} d_i x^i \text{ where } d_i = \sum_{j+t=i} a_j b_t x^i$$

Thus using that f is a homomorphism we see that $\bar{f}(a(x)b(x))$ the steps below.

$$\begin{aligned}
\bar{f}(a(x)b(x)) = \bar{f}(d(x)) &= \sum_{i=0}^{n+m} f(d_i)x^i, \\
&= \sum_{i=0}^{n+m} f\left(\sum_{j+t=i} (a_j b_t)\right) x^i = \sum_{i=0}^{n+m} \left(\sum_{j+t=i} f(a_j b_t)\right) x^i, \\
&= \sum_{i=0}^{n+m} \left(\sum_{j+t=i} f(a_j) f(b_t)\right) x^i = \bar{f}(a(x))\bar{f}(b(x)).
\end{aligned}$$

Proof of additivity I agree that this should be left as an exercise, so let's do that.

Thus $\bar{f}$ is a homomorphism. □

Theorem 30. *Let A, K be commutative rings with unity, and suppose that $f : A \to K$ is an isomorphism. Then the extension $\bar{f} : A[x] \to K[x]$ is also an isomorphism.*

Proof Sketch. Don't try to use the first isomorphism theorem here, instead proceed by the definitions of surjective, injective, additive, and multiplicative functions. The author includes the following hint:

Don't forget that in order for polynomials to be equal they must have identical coefficients. When assuming $\bar{f}(a(x)) = \bar{f}(b(x))$ for the proof of injectivity, you have that the coefficients are indeed identical. What are the coefficients? □

7.3 Polynomial Functions and Roots

Definition 33. *Let A be a commutative ring with unity and $a(x) \in A[x]$ with $a(x) \neq 0(x)$. If $c \in A$ and $\deg(a(x)) = n$, we define the element $a(c) \in A$ as follows:*

$$a(c) = a_0 +_A (a_1 \cdot_A c) +_A (a_2 \cdot_A c^2) +_A \cdots +_A (a_n \cdot_A c^n).$$

If $a(x) = 0(x)$ we say $a(c) = 0_A$ for all $c \in A$.

Theorem 35. *Let A be an integral domain. The substitution function $h_c : A[x] \to A$ defined by $h_c(a(x)) = a(c))$ is a ring homomorphism.*

Proof. Let h_c, $a(x)$, $b(x)$ be as defined in Theorem 7.35. We will show that h_c is additive,

$$\begin{aligned}
h_c(a(x) + b(x)) &= h_c\left(\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{m} b_i x^i\right), \\
&= h_c\left(\sum_{i=0}^{\max(n,m)} (a_i + b_i) x^i\right), \\
&= \sum_{i=0}^{\max(n,m)} (a_i + b_i) c^i, \\
&= \sum_{i=0}^{n} a_i c^i + \sum_{i=0}^{m} b_i c^i, \\
&= a(c) + b(c), \\
&= h_c(a(x)) + h_c(b(x)).
\end{aligned}$$

Observe that A must be an integral domain in order for each of the terms to 'stay alive' through the process of adding all of the terms together, and then pulling them apart again. Thus, h_c is additive, as we aimed to show. □

Definition 37. *Let A be a commutative ring with unity, $c \in A$, and $a(x) \in A[x]$ $a(x) \neq 0(x)$. We say that c is a root of the polynomial $a(x)$ exactly when $a(c) = 0_A$. We do not say any element of A is a root of $0(x)$ even though $0(c) = 0_A$ for each $c \in A$.*

8 Factoring Polynomials

8.1 Factors and Irreducible Polynomials

Commentary In Chapter 8 we focus on factoring polynomials, which devolves into arguments about irreducibility, associates, roots, and factors. Section 8.1 helps us define these concepts and introduces their elementary properties. Section 8.2 continues this line of inquiry in the direction of finding the roots and factors of a polynomial. Section 8.3 focuses specifically on the question of factoring polynomials in $\mathbb{Q}$.

Definition 1. *Let A be a commutative ring with unity and $a(x), d(x) \in A[x]$. We say that $a(x)$ is a factor of $d(x)$ if there exists a polynomial $b(x) \in A[x]$ with $d(x) = a(x)b(x)$.*

Definition 4. *Let A be an integral domain. Polynomials $a(x), b(x) \in A[x]$ are called associates if there is a nonzero element $c \in A$ so that the constant polynomial $c(x) = c$ has $a(x) = c(x)b(x)$.*

We will frequently write $a(x) = cb(x)$ instead of first defining the constant polynomial $c(x) = c$.

Theorem 5. *Let A be an integral domain and suppose $a(x), b(x) \in A[x]$ are associates. Then $c \in A$ is a root of $a(x)$ if and only if c is a root of $b(x)$.*

Proof Sketch. This should be a very accessible proof for my future self, the author includes a useful hint:

Use Theorem 7.35 (the evaluation function is a homomorphism) to help, and that A is an integral domain (what does that mean?). □

Definition 7. *Let A be an integral domain with $a(x) \in A[x]$ and $\deg(a(x)) > 0$. We say that $a(x)$ is irreducible over A if every factor of $a(x)$ in $A[x]$ is either a constant polynomial or an associate of $a(x)$. If instead a nonconstant factor of $a(x)$ which is not an associate of $a(x)$ exists in $A[x]$, we say that $a(x)$ is reducible over A.*

Theorem 8. *Let K be a field and suppose $a(x), b(x) \in K[x]$ are associates. The polynomial $a(x)$ is irreducible over K if and only if $b(x)$ is irreducible over K.*

Proof. Let K, $a(x)$, and $b(x)$ be as above.

$\Rightarrow$) Assume $a(x)$ is irreducible over K, and suppose by way of contradiction that $b(x)$ is reducible over K. Then we know there exists polynomials $d(x)$,$f(x) \in K[x]$ such that $b(x) = d(x)f(x)$. And since $a(x)$ and $b(x)$ are associates we can write $a(x) = cb(x) = c[d(x)f(x)]$ ↯

This implies that $a(x)$, which we assumed to be irreducible over K, has factors in $K[x]$, a contradiction. A similar argument can be used to prove the converse. □

Theorem 9. *Let K be a field. Every polynomial in $K[x]$ of degree 1 is irreducible over K.*

Proof. Let K be a field and $a(x) \in K[x]$ such that $\deg a(x) = 1$. Since K is a field $K[x]$ is an integral domain and thus the degree of polynomials is additive in $K[x]$. We can write $a(x) = b(x)c(x)$, and since $\deg a(x) = 1$, we know that either $\beta = \deg b(x) = 1$ and $\gamma = \deg c(x) = 0$, or the other way around. This means that we can only factor $a(x)$ into associates, which is the definition of being irreducible.

Hence, for a field K, every polynomial in $K[x]$ of degree 1 is irreducible over K. □

Theorem 11. *Suppose K is a field, and $p(x) \in K[x]$. If $p(x)$ is irreducible over K then $\langle p(x) \rangle$ is a maximal ideal of $K[x]$.*

Proof. Assume K is a field, $p(x) \in K[x]$, and $p(x)$ is irreducible over K. Let $S = \langle p(x) \rangle$, and we will show S is a maximal ideal. Assume instead there is an ideal T in $K[x]$ with $S \subset T \subset K[x]$. Notice that as $\deg(p(x)) > 0$ and $p(x) \in S$ then $S \neq \{0(x)\}$ and $T \neq \{0(x)\}$.

By Theorem 7.26 T must be a principal ideal. Thus there exists $b(x) \in T$ with $T = \langle b(x) \rangle$ and $b(x) \neq 0(x)$. Now $p(x) \in T$ and so $p(x) = b(x)q(x)$ for some $q(x) \in K[x]$. But $p(x)$ is irreducible over K and $b(x)$ is a factor of $p(x)$, so either $b(x)$ is an associate of $p(x)$ or $b(x)$ is a constant polynomial.

Suppose first that $b(x)$ is a constant polynomial, $b(x) = b_0$ with $b_0 \neq 0_K$. Since K is a field, the polynomial $s(x) = b_0^{-1}$ is in $K[x]$ and $b(x)s(x) \in T$. But $b(x)s(x) = 1(x)$ so by Theorem 5.12 we have $T = K[x]$ contradicting the choice of T.

Thus $b(x)$ must be an associate of $p(x)$ instead, and there is a nonzero $c \in K$ with $p(x) = cb(x)$. K is a field, so we know $c^{-1} \in K$ which tells us $c^{-1}p(x) = b(x)$ and thus $b(x) \in S$. Since S is an ideal we now know that every element of T, of the form $b(x)w(x)$, is also in S and $T = S$ which again contradicts the choice of T. Every possibility has lead us to a contradiction, so no such T can exist, and $S = \langle p(x) \rangle$ is a maximal ideal of $K[x]$. □

Commentary The following theorem tells us that polynomials that are irreducible over a ring of coefficients K act like prime numbers in the polynomial ring $K[x]$.

Theorem 12. *Let K be a field, and assume that $p(x) \in K[x]$ is irreducible over K. If $a(x), b(x) \in K[x]$ and $p(x)$ is a factor of the product $a(x)b(x)$, then $p(x)$ is a factor of at least one of $a(x)$ or $b(x)$.*

Proof Sketch. While this theorem is dripping with Number Theory, the proof is mostly reliant on facts about principal and maximal ideals. The author includes this hint:

Use Theorems 8.11 and 6.23. Remember that $b(x) \in \langle p(x) \rangle$ means that $p(x)$ is a factor of $b(x)$.

To check the validity of your proof, a detailed answer can be found in the solutions to Homework 2. If you have access to this some years after writing it, you'd better have access to your old homeworks, and their solutions. □

Theorem 14. *Let K and E be fields, and suppose that $\bar{f} : K \to E$ is an isomorphism. The polynomial $p(x) \in K[x]$ is irreducible over K if and only if $\langle p(x) \rangle$ is irreducible over E.*

Proof. Let K and E be fields, $f : K \to E$ an isomorphism, and $p(x) \in K[x]$. $\Rightarrow$) Assume $p(x)$ is irreducible over K, and for a contradiction suppose $\bar{f}(p(x))$ is reducible over E. Thus there exist polynomials $q(x), r(x) \in E[x]$ with $\langle p(x) \rangle = q(x)r(x)$, $\deg(q(x)) > 0$, and $\deg(r(x)) > 0$.

By Theorem 7.30 $\bar{f}$ is an isomorphism, and thus onto, so we must have $s(x), t(x) \in K[x]$ with $\bar{f}(s(x)) = q(x)$, and $\bar{f}(t(x)) = r(x)$. Also $\deg(s(x)) = \deg(q(x))$, and $\deg(r(x)) = \deg(t(x))$ (an exercise in Chapter 7). Since $\bar{f}$ is a homomorphism we have the following equalities:

$$\bar{f}(s(x)t(x)) = \bar{f}(s(x))\bar{f}(t(x)) = q(x)r(x) = \bar{f}(p(x)).$$

But $\bar{f}$ is one to one so $p(x) = s(x)t(x)$. Since $\deg(s(x)) > 0$ and $\deg(t(x)) > 0$ this contradicts that $p(x)$ is irreducible over K. Thus $\langle p(x) \rangle$ is irreducible over E.

$\Leftarrow$) Suppose that $b(x) = x - c$ is a factor of $a(x)$, we will show that $c \in K$ is a root of $a(x)$. Since $b(x)$ is a factor of $a(x)$, we can write $a(x) = b(x)d(x)$ for some polynomial $d(x)$. Further, since K is a field, $K[x]$ is an integral domain and the zero product property works like we'd like it to, so we have $a(c) = (c - c)d(c) = 0$, hence c is a root of $a(x)$. □

8.2 Roots and Factors

Theorem 15. *Let K be a field and $a(x) \in K[x]$ with $a(x) \neq 0(x)$. The element $c \in K$ is a root of $a(x)$ if and only if $b(x) = -c + x$ is a factor of $a(x)$.*

Proof Sketch. Use polynomial long division, and the evaluation homomorphism for the forward direction, you proved the backwards direction in Homework 3. □

Theorem 17. *Suppose K is a field and $a(x) \in K[x]$ with $a(x) \neq 0(x)$. If the distinct elements $c_1, c_2, \ldots, c_n \in K$ are all roots of $a(x)$, then the product $b(x) = (-c_1 + x)(-c_2 + x) \cdots (-c_n + x)$ is a factor of $a(x)$.*

Proof Sketch. Use induction, and in so doing use Theorem 8.15 a bunch of times. □

Theorem 19. *Let K be a field. If $c_1, c_2, \ldots, c_n \in K$ are distinct roots of the nonzero polynomial $a(x) \in K[x]$, then $\deg(a(x)) \geq n$.*

Proof. Let K, $a(x)$ be as above. By Theorem 8.17 we can write $a(x) = b(x)f(x)$ where $f(x) = \prod_{i=1}^{n}(x - c_i)$ for distinct roots $c_i \in K$. Since K is a field, $K[x]$ is an integral domain and degree is additive for elements of $K[x]$. Let $\deg a(x) = \alpha$, $\deg b(x) = \beta$, $\deg f(x) = \eta$. Its clear that $\eta = n$, and by the same reasoning that allows us to conclude that, we can also surmise $\alpha \geq \eta$, hence $\deg(a(x)) \geq n$, as desired. □

Theorem 20. *Suppose K is a field and $a(x) \in K[x]$. If $\deg(a(x)) > 0$ then there exist a positive integer m and polynomials $b_1(x), b_2(x), \ldots, b_m(x) \in K[x]$ which are irreducible over K and $a(x) = b_1(x)b_2(x) \cdots b_m(x)$.*

Commentary This let's use write any polynomial as a product of its irreducible polynomial factors, just as we can write integers as a product of its prime factors. The proof in the book is fairly readable.

Theorem 22. *Let K be a field and $a(x) \in K[x]$ with $\deg(a(x)) = 2$ or $\deg(a(x)) = 3$. The polynomial $a(x)$ is reducible over K if and only if $a(x)$ has a root in K.*

Commentary This is one of the few pieces of commentary that I feel is actually useful. This theorem is exceedingly important, a frequent mistake (that you made a lot when first learning this material) is that one assumes *any* polynomial with no roots over a field is therefore irreducible, this theorem tells us that that is only the case for polynomials with degree no greater than three. By definition constants and linear polynomials are irreducible, so this covers the only other cases.

Bottom line: If its degree four or higher, you probably have some work to do.

Definition 24. *Let K be a field and $a(x) \in K[x]$. Suppose $a(x) \neq 0(x)$, with $\deg(a(x)) = n$. The polynomial $a(x)$ is **monic** if $a_n = 1_K$.*

Definition 26. *Let K be a field and $a(x) \in K$ with $a(x) \neq 0(x)$. Suppose $c \in K$ is a root of $a(x)$. If there is an integer $m > 0$ for which the polynomial $b(x) = (-c + x)^m$ is a factor of $a(x)$ but $d(x) = (-c + x)^{m+1}$ is not a factor of $a(x)$, then we say that c is a root of $a(x)$ with multiplicity m.*

Theorem 27. *Let K be a field and $a(x) \in K[x]$ with $a(x) \neq 0(x)$. If $\deg(a(x)) = n$ then there can be at most n distinct roots of $a(x)$ in K.*

Proof. Let K be a field and $a(x) \in K[x]$ with $a(x) \neq 0(x)$, and assume that $\deg a(x) = n$. Since $\deg a(x) = n$, we can write $a(x) = b(x)f(x)$ for some polynomials $b(x)$ and $f(x) = \prod_{i=1}^{n}(x - c_i)$, each of which is an element of $K[x]$, where $c_i \in K$ are the roots of $a(x)$. Notice that the linear factors that comprise $f(x)$ each has degree 1, thus $f(x) = \prod_{i=1}^{n}(x - c_i)$ has degree n, as K is a field and $K[x]$ and integral domain. That tells us that the only option for $b(x)$ is a constant polynomial with degree 0. This implies that $f(x)$ takes into account each of the distinct roots of $a(x)$, hence $a(x)$ has at most n distinct roots in K. □

Theorem 28. *Let K be an infinite field. If $a(x), b(x) \in K[x]$, and $a(x) \neq b(x)$, then there must exist some $c \neq K$ for which $a(c) \neq b(c)$.*

Proof Sketch. This is a fairly straightforward concept that was discussed in Lecture 5 on 19 January, 2018; it can be found on page 177 of your notes. Again, if you don't have your old notes, but you have this document, something has gone awry. □

8.3 Factorization over $\mathbb{Q}$

Commentary The following theorems are tools with which we can factor polynomials over the rationals, the fact that the tools are few in number and generally not that powerful are an indication of how difficult it is to factor over an infinite field, and offers a quick-and-dirty explanation as to why finding the roots of the Riemann zeta function is so damned hard (and worth a million dollars).

Theorem 29. *If $a(x) \in \mathbb{Q}[x]$ with $a(x) \neq 0(x)$ then there is a polynomial $b(x) \in \mathbb{Z}[x]$ with $\deg(a(x)) = \deg(b(x))$ which has exactly the same rational roots as $a(x)$.*

Theorem 31 (The Rational Roots Theorem)**.** *Let $a(x) \in \mathbb{Z}[x]$ with $a(x) \neq 0(x)$ and $\deg(a(x)) = n$. If the rational number $\frac{s}{t}$ ($s, t \in \mathbb{Z}$ with no common prime factors and $t \neq 0$) is a root of $a(x)$ then s must evenly divide a_0 and t must evenly divide a_n.*

Theorem 33. *If $a(x) \in Z[x]$ and $a(x) = b(x)c(x)$ with $b(x), c(x) \in \mathbb{Q}[x]$, $\deg(b(x)) > 0$, and $\deg(c(x)) > 0$, then there exist polynomials $u(x), w(x) \in \mathbb{Z}[x]$ with $a(x) = u(x)w(x)$, $\deg(u(x)) > 0$, and $\deg(w(x)) > 0$.*

Theorem 35 (Eisenstein's Criterion)**.** *Suppose $a(x) \in \mathbb{Z}[x]$ and $\deg(a(x)) = n$ with $n > 0$. If there exists a prime number p which divides coefficients $a_0, a_1, \ldots, a_{n-1}$ but not a_n, and p^2 does not divide a_0, then $a(x)$ is irreducible over $\mathbb{Q}$.*

Theorem 37. *Suppose $a(x) \in \mathbb{Z}[x]$ is a monic polynomial and $\deg(a(x)) = k$ with $k > 0$. If there exists $n > 1$ so that $\bar{f}_n(a(x))$ is irreducible in $\mathbb{Z}_n[x]$ then $a(x)$ is also irreducible in $\mathbb{Z}[x]$.*

9 Extension Fields

Commentary In Chapter 9 we turn our attention to Fields. When considering groups and rings, we examined their sub-objects and sub-structures. Here, we flip the script and consider *field extensions*, basically going in the other direction. Given a field, what other fields (aside from itself) is the field a sub-field of? This leads us to the subject of Minimum Polynomials in §9.2, Algebraic Extensions in §9.3, and Root Fields in §9.4.

I have nothing useful or intelligent to say about the content from Chapter 9, I would refer anyone looking to enhance their understanding of the material to the examples in the texbook, the lecture notes, or the myriad of online resources for students of modern algebra.

9.1 Extension Field

Definition 1. *Suppose that K and E are fields with $K \subseteq E$. If for all $a, b \in K$ we have $a +_K b = a +_E b$ and $a \cdot_K b = a \cdot_E b$, then K is a subfield of E or E is an extension field of K.*

Definition 2. *Suppose E is an extension field of K, and $c \in E$*

(i) If there exists $a(x) \in K[x]$ with $a(x) \neq 0(x)$ and $a(c) = 0_E$, then c is ***algebraic over*** *K.*

(ii) If for every nonzero $a(x) \in K[x]$ we have $a(c) \neq 0_E$, then c is ***transcendental over*** *K.*

Theorem 4. *Suppose E is an extension field of K, $a(x) \in K[x]$, and there is $c \in E$ with $a(c) = 0_E$.*

(i) If $\deg(a(x)) = 1$, then $c \in K$.

(ii) If $a(x)$ is irreducible over K and $\deg(a(x)) > 1$, then $c \notin K$

Theorem 5. *Suppose K is a field. E is an extension field of K and $c \in E$. IF c is algebraic over K, then there exists a field $K(c)$ ("**K adjoin c**") with:*

(i) $K \subseteq K(c) \subseteq E$.

(ii) $c \in K(c)$.

(iii) For any subfield S of E with $K \subseteq S$ and $c \in S$ we have $K(c) \subseteq S$.

Theorem 7. *Let K be a field and assume $a(x) \in K[x]$ is irreducible over K. Then there exists a field E so that E is an extension field of K and $a(x)$ has a root in E.*

9.2 Minimum Polynomial

Theorem 9. *If K is a field, E is an extension field of K, and $c \in E$ is algebraic over K, then there is a* ***unique monic*** *polynomial $p(x) \in K[x]$ that is irreducible over K and has c as a root.*

Definition 10. *Let K be a field, E and extension field of K, and $c \in E$ algebraic over K. The unique monic polynomial $p(x) \in K[x]$ that is irreducible over K and has c as a root is called* ***the minimum polynomial*** *for c over K.*

Theorem 12. *Suppose K be a field, E and extension field of K, and $c \in E$ algebraic over K with minimum polynomial $p(x) \in K[x]$.*

(i) Using the homomorphism $f_c : K[x] \to E$ as defined in Theorem 9.5, $\ker(f_c) = \langle p(x) \rangle$.

(ii) If $b(x) \in K[x]$ is a nonzero polynomial with $b(c) =)_E$, then $b(x) = p(x)q(x)$ for some $q(x) \in K[x]$.

Theorem 13. *Suppose K be a field, E and extension field of K, and $c \in E$ algebraic over K. If $p(x)$ is the minimum polynomial for c over K, and $\deg(p(x)) = n$, then:*

$$K(c) = \{a(c) : a(x) \in K[x] \text{ and either } a(x) = 0(x) \text{ or } \deg(a(x)) < n\}.$$

9.3 Algebraic Extensions

Definition 16. *Let K be a field and E an extension field of K. If every element of E is algebraic over K we say that E is an* ***algebraic extension*** *of K.*

Definition 17. *Let K be a field and E an extension field of K. A nonempty subset of E, $B = \{u_1, u_2, \ldots, u_m\}$ is called a* ***basis for E over K*** *when the following hold:*

(i) For every element $s \in E$ there exist $a_1, a_2, \ldots, a_m \in K$ so that $s = a_1u_1 + a_2u_2 + \ldots a_mu_m$ (B spans E over K).

(ii) If $a_1, a_2, \ldots, a_m \in K$ with $a_1u_1 + a_2u_2 + \ldots a_mu_m = 0_E$ then $a_i = 0_K$ for all $i = 1, \ldots, m$ (B is independent over K).

*If there exist m elements of E that form a basis for E over K we say E is a **finite extension** of K of degree m, and write $[E : K] = m$.*

Theorem 19. *Let K be a field and E an extension field of K.*

(i) Every basis for E over K has the same cardinality.

(ii) Every subset of E that spans E contains a basis for E over K.

Theorem 20. *Suppose K is a field, c is algebraic over K with minimum polynomial $p(x)$, and $\deg(p(x)) = n$. Then the set $B = \{1_K, c, c^2, \ldots, c^{n-1}\}$ is a bsis for $K(c)$ over K and $[K(c) : K] = \deg(p(x))$.*

Theorem 21. *Let K be a field and E an extension field of K with $[E : K] = n$ for some $n > 0$. Then E is an algebraic extension of K.*

Theorem 22. *Suppose that K is a field and L is a finite extension of K. If E is a finite extension of L, then E is also a finite extension of K and $[E : K] = [E : L][L : K]$.*