DRAFT – Commentary Portfolio – DRAFT

Student #1091

January 20, 2018

Contents

Chapter 7

Polynomials over a Ring

7.1 Polynomials over a Ring

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 $0 \leq t \leq m$.

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 $A[x]$.*

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

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

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.*

7.2 Properties of Polynomial Rings

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

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 $\deg(a(x)b(x)) = n + m$.*

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

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 $r(x) = 0(x)$.*

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

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.*

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

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.*

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.*

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 $c \in A$.*

Chapter 8

Factoring Polynomials

8.1 Factors and Irreducible Polynomials

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 $b(x)$.*

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.*

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

Theorem 10. *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 $K[x]$.*

Theorem 11. *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 $b(x)$.*

Theorem 12. *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.*

8.2 Roots and Factors

Theorem 13. *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 $a(x)$.*

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 $a(x)$.*

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 $\deg(a(x)) \geq n$.*

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 $a(x) = b_1(x)b_2(x) \cdots b_m(x)$.*

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.*

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.*

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 $a(c) \neq b(c)$.*