# **Section IV.22.** Rings of Polynomials

**Note.** In this section we set the stage for addressing topics from classical algebra (namely, finding the zeros of a polynomial) in the setting of modern algebra (groups, rings, and fields—rings, in this section). To do so, we must keep all "items of interest" (i.e., polynomials) as elements of our modern algebraic structures. As the name of the section suggests, we build a ring out of polynomials.

**Note IV.22.A.** We'll use the symbol "$x$" to create polynomials with coefficients chosen from some ring. The parameter $x$ is referred to as an *indeterminate*, as opposed to a variable. Indeterminate $x$ is just a symbol that allows us to create polynomials. Strictly speaking, we do not substitute values in for $x$, but instead we will use a homomorphism to map a polynomial onto a "value" in a ring containing the coefficients. In this way, we are always dealing with elements of rings (and often elements of a field).

**Definition 22.1.** Let $R$ be a ring. A *polynomial* $f(x)$ with coefficients in $R$ is an infinite formal series

$$\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots$$

where $a_i \in R$ and $a_i = 0$ for all but a finite number of values of $i$. The $a_i$ are *coefficients* of $f(x)$. If for some $i \geq 0$ it is true that $a_i \neq 0$, then the largest such value of $i$ is the *degree* of $f(x)$. If all $a_i = 0$, then the degree of $f(x)$ is undefined.

If $a_i = 0$ for all $i \in \mathbb{N}$, then $f(x)$ is called a *constant polynomial*. We denote the set of all polynomials with coefficients in $R$ as $R[x]$.

**Note.** We use a notation consistent with your previous experiences. If $f(x)$ is of degree $n$ we may write $f(x)$ as $a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$, instead of as an infinite sum. If $R$ has unity $1 \neq 0$, we write $x^k$ to represent $1x^k$. If some $a_i = 0$ then we omit the term $a_i x^i = 0x^i$ when writing the formal sums. For example, if $f(x) = 0 + 1x + 1x^2 + 0x^3 + 1x^4 + 0x^5 + 0x^6 + 0x^7 + \cdots$ then we write $f(x)$ as $x + x^2 + x^4$.

**Note.** You have seen infinite formal sums in Calculus 2 (MATH 1920) as power series (see my online Calculus 2 notes on Section 10.7. Power Series). Of course, your main concern with a power series is the values of $x$ for which the series converges. However, notice that a polynomial is an infinite formal sum, but in practice it is only a finite sum since all but a finite number of the $a_i$ are 0. So we have no concerns over convergence or divergence (that is a problem for Analysis 1 and 2 [MATH 4217/5217 and 4227/5227]).

**Definition.** We define $+$ and $\cdot$ on $R[x]$ as follows. Let $f(x), g(x) \in R[x]$ where

$$f(x) = \sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots,$$

$$g(x) = \sum_{i=0}^{\infty} b_i x^i = b_0 + b_1 x + b_2 x^2 + \cdots + b_n x^n + \cdots.$$

Define the sum $f(x) + g(x)$ as

$$f(x) + g(x) = \sum_{i=0}^{\infty} c_i x^i = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n + \cdots$$

where $c_i = a_i + b_i$, and define the product $f(x) \cdot g(x)$ as

$$f(x) \cdot g(x) = \sum_{i=0}^{\infty} d_i x^i = d_0 + d_1 x + d_2 x^2 + \cdots + d_n x^n + \cdots$$

where $d_n = \displaystyle\sum_{i=0}^{n} a_i b_{n-i}$.

**Note.** Since all but a finite number of the $a_i$s and $b_i$s are 0, than all but a finite number of the $c_i$s and $d_i$s are 0, and hence the sum and product of $f(x)$ and $g(x)$ are in fact actually elements of $R[x]$.

**Theorem 22.2.** The set $R[x]$ of all polynomials in an indeterminate $x$ with coefficients in a ring $R$ is a ring under polynomial addition and multiplication as defined above. If $R$ is commutative, then so is $R[x]$, and if $R$ has unity $1 \neq 0$, then 1 (a constant polynomial) is also unity for $R[x]$.

**Example.** $\mathbb{Z}[x]$ is the ring of all polynomials with integer coefficients. The zeros of all of these polynomials (in $\mathbb{R}$) make up the field of *algebraic numbers.*

**Note IV.22.B.** Since $R[x]$ is a ring, we can introduce a second indeterminate $y$ and define the ring $(R[x])[y]$, the ring of polynomials in $y$ with coefficients in $R[x]$. Not surprisingly, any element of $(R[x])[y]$ can be rewritten as a polynomial in $x$

with coefficients from $R[y]$ (just collect together the powers of $x$). This allows us to refer to $R[x, y]$, the *ring of polynomials in two indeterminates* $x$ and $y$ with coefficients in $R$. We can also refer to $R[x_1, x_2, \ldots, x_n]$, the ring of polynomials in $n$ indeterminates $x_1, x_2, \ldots, x_n$ with coefficients in $R$. However, our study will be restricted to single indeterminate polynomials.

**Note IV.22.C.** If $D$ is an integral domain, then so is $D[x]$ (we need only show that $D[x]$ has no zero divisors—this is Exercise 22.24). So by Theorem 21.5, there is a field of quotients of $D[x]$, which we denote as $F(x)$, where every element of $F(x)$ is a quotient of elements of $D[x]$: $q(x) \in F(x)$ implies $q(x) = f(x) /_F g(x)$ for some $f(x), g(x) \in D[x]$, $g(x) \neq 0$. $F(x)$ is called the *field of rational functions* in indeterminate $x$ with coefficients from $D$ (we can also start with a field $F$ instead of an integral domain $D$).

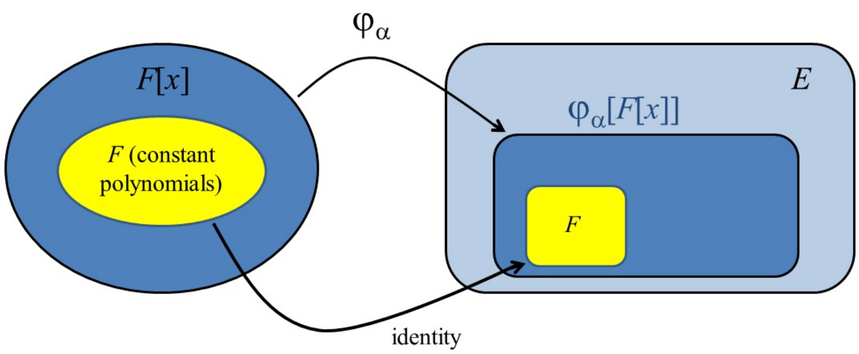
**Note.** The following result allows us to indirectly deal with substituting values into a polynomial. This is accomplished using a homomorphism, since we are restricted to dealing simply with rings and mappings. The idea presented here is fundamental in the study of polynomials which is to follow (briefly in Section IV.23 and in some more detail in Part X).

**Theorem 22.4. The Evaluation Homomorphism for Field Theory.**
Let $F$ be a subfield of a field $E$, let $\alpha \in E$, and let $x$ be an indeterminate. The map $\varphi_\alpha : F[x] \to E$ defined by

$$\varphi_\alpha(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n$$

where $a_0+a_1x+a_2x^2+\cdots+a_nx^n \in F[x]$, is a homomorphism of $F[x]$ into $E$. Also, $\varphi_\alpha(x) = \alpha$, and $\varphi_\alpha$ maps $F$ isomorphically by the identity map; that is, $\varphi_\alpha(a) = a$ for $a \in F$. The homomorphism $\varphi_\alpha$ is the *evaluation at* $\alpha$.

**Note.** Schematically, we have (for fixed $\alpha \in E$):




On the left, $F$ is a subring of $F[x]$ (remember that there are not in general inverses of elements of $F[x]$, for example $f(x) = x$ has no multiplicative inverse in $F[x]$, so $F[x]$ is not a field). On the right, $F$ is a subfield of $E$. No claim is mentioned in the theorem about the structure of $\varphi_\alpha[F[x]]$, so it may not be a field or even a ring.

**Note.** Theorem 22.4 holds if $F$ and $E$ are commutative rings with unity instead of fields. However, it is the case of fields on which our future studies will be centered.

**Example 22.6.** Let $F$ be $\mathbb{Q}$ and $E$ be $\mathbb{R}$ in Theorem 22.4. Consider $\varphi_0 : \mathbb{Q}[x] \to \mathbb{R}$. We have

$$\varphi_0(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) = a_0 + a_1 0 + a_2 0^2 + \cdots + a_n 0^n = a_0.$$

So $\varphi_0$ maps a polynomial in $\mathbb{Q}[x]$ to the constant term. As sets, $\varphi_0[\mathbb{Q}[x]] = \mathbb{Q}$.

**Example 22.8.** Let $F$ be $\mathbb{Q}$ and $E$ be $\mathbb{C}$ in Theorem 22.4. Consider $\varphi_i : \mathbb{Q}[x] \to \mathbb{C}$. Then

$$\varphi_i(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) = a_0 + a_1 i + a_2 i^2 + \cdots + a_n i^n.$$

Notice that $\varphi_i(x^2 + 1) = i^2 + 1 = -1 + 1 = 0$ and so $x^2 + 1 \in \mathrm{Ker}(\varphi_i)$.

**Definition 22.10.** Let $F$ be a subfield of a field $E$, and let $\alpha \in E$. Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in F[x]$ and let $\varphi_\alpha : F[x] \to E$ be the evaluation homomorphism of Theorem 22.4. We denote

$$\varphi_\alpha(f(x)) = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n$$

as $f(\alpha)$. If $f(\alpha) = 0$, then $\alpha$ is a *zero* of $f(x)$.

**Note IV.22.D.** Finding the zeros of $f(x) \in F[x]$ is equivalent to finding $\alpha \in E$ such that $\varphi_\alpha(f) = 0$. So the classical algebra problem of solving a polynomial equation has been converted into a question about a mapping (a homomorphism) in the modern algebra setting. Remember that it is quite challenging to solve polynomial equations. However, the equipment of modern algebra will tell us when a polynomial equation can be solved algebraically and how to solve it (this is accomplished in Galois theory which is lightly touched on in Part X).

**Note IV.22.E.** The text paraphrases the **basic goal** of this endeavor as "to show that given any polynomial of degree $n \geq 1$, where the coefficients of the polynomial may be from any field, we can find a zero of this polynomial in some field containing the given field." This is accomplished after Sections V.26 and V.27 ("Homomorphisms and Factor Rings" and "Prime and Maximal Ideals") in Section VI.29 ("Introduction to Extension Fields") in *Kronecker's Theorem*: Let $F$ be a field and let $f(x)$ be a nonconstant polynomial in $F[x]$. Then there exists an extension field $E$ of $F$ and an $\alpha \in E$ such that $f(\alpha) = 0$.

**Note.** The book motivates the basic goal by showing that $x^2 - 2 \in \mathbb{Q}[x]$ has no zero in $\mathbb{Q}$. Of course, $x^2 + 1 \in \mathbb{R}[x]$ has no zero in $\mathbb{R}[x]$. However, any polynomial $p(x) \in \mathbb{C}[x]$ has a zero in $\mathbb{C}$. That is, $\mathbb{C}$ is algebraically closed. This is the Fundamental Theorem of Algebra (Theorem 31.18 of Section VI.31. Algebraic Extensions).

*Revised: 7/14/2023*