# Algebraic Theory I

Thomas Fleming

November 17, 2021

## Contents



# 1 Polynomial Rings

## Lecture 35: Polynomials

Mon 15 Nov 2021 11:32

**Definition 1.1** (Polynomial Ring)**.** Let $R$ be a commutative ring and we define $R[X]$ to be the ring of polynomials in the variable $x$ with coefficients from $R$ defined as follows.
An element $f \in R[X]$ has the form

$$f = a_0 + a_1 x + \ldots + a_n x^n$$

for some $n \geq 0$ and each $a_i \in R$. This is a formal sum in the sense that two polynomials

$$\begin{aligned} f &= a_0 + a_1 x + \ldots + a_n x^n \\ g &= b_0 + b_1 x + \ldots b_m x^m \end{aligned}$$

have $f = g$ if and only if $a_i = b_i$ for every $i$.
For the polynomial $f$, we call $a_0$ the **constant term** and $a_n$ to be the **leading coefficient** and $n$ to be the **degree**, denoted $\deg(f) = n$ .
For the polynomial $f = 0$, we specifically define $\deg(f) = -1$. For all other constant polynomials $g$, we define $\deg(g) = 0$.

**Remark.** Occasionally, we will write $f = \sum_{i=0}^{\infty} a_i x^i$ with almost every $a_i = 0$. With this form we see elements of $R[X]$ are in a bijective correspondence with finite support tuples from $R^{\mathbb{N}}$.

We see $R[X]$ forms a ring with two polynomials $f, g \in R[X]$ as defined earlier having sum

$$(f+g) = \sum_{i=0}^{\infty} (a_i + b_i) x^i$$

and

$$fg = \sum_{i=0}^{\infty} a_i x^i \sum_{j=0}^{\infty} b_j x^j = \sum_{n=0}^{\infty} \sum_{\substack{i,j \\ i+j=n}} a_i b_j x^n.$$

**Definition 1.2** (Multivariate Polynomial Rings)**.** We define a **multivariate polynomial ring** $R[x_1, \ldots, x_n] = (R[x_1, \ldots, x_{n-1}])[x_n]$ with addition and multiplication defined similarly. It is worth noting that while degree and constants are well defined, the leading coefficient may be poorly defined without adding extra constraints.

**Definition 1.3** (Projected Degree)**.** For a multivariate polynomial $f \in R[x_1, \ldots, x_n]$ we define $\deg(f)_{x_i}$ to be the degree when considered only in the variable $x_i$.

**Remark.** It is of note that polynomials are more formal objects and not necessarily functions. The distinction is mostly moot, but we can induce a function from a polynomial by defining a function

$$\begin{aligned} f : R &\longrightarrow R \\ b &\longmapsto f(b) = \sum_{i=0}^{\infty} a_i b^i. \end{aligned}$$

The point of this distinction is that polynomials over finite (or otherwise non-standard spaces) may not be distinct. For example $x \mapsto x^5 - x$ and $x \mapsto 0$ are completely equivalent in $\mathbb{F}_5$. This, of course, cannot happen over $\mathbb{R}$ unless the coefficients are precisely equal.

We can construct a function in a different way as follows:

**Definition 1.4** (Evaluation Map)**.** Fixing $b \in R$ we define the **evaluation map** on $R[x]$ as

$$\begin{aligned} \mathrm{ev}_b : R[x] &\longrightarrow R \\ f &\longmapsto \mathrm{ev}_b(f) = f(b). \end{aligned}$$

We find this map to be a ring homomorphism, essentially compressing $R[x]$ down into $R$.

## Lecture 36: Polynomials (2)

Mon 07 May 2018 03:55

**Recall.** For a commutative ring $R$, we define the polynomial ring $R[x_1, \ldots, x_n]$ as formal sums of powers of $x_i$ with coefficients in $R$.

Moreover, if we have two commutative rings $R, R'$ with a ring homomoprhism $\varphi : R \to \overline{\mathbb{R}}$ , then there is a complementary ring homomorphism extending to the polynomial ring:

$$\begin{aligned}\overline{\varphi} : R[x] &\longrightarrow \overline{\mathbb{R}}[x]\\ \sum_{i=0}^{\infty} \alpha_i x^i &\longmapsto \sum_{i=0}^{\infty} \varphi(a_i) x^i.\end{aligned}$$

**Definition 1.5** (Map Space)**.** Now, define $\mathrm{Map}(Y \to R)$ to be the set of all maps $f : Y \to R$ with $R$ being a commutative ring and $Y$ being an arbitrary set. We equip $\mathrm{Map}(Y \to R)$ with pointwise operations $\times, +$ such that

$$\begin{aligned}(f+g)(x) &= f(x) + g(x)\\ (fg)(x) &= f(x)\, g(x)\end{aligned}$$

.

These operations induce a ring over $\mathrm{Map}(Y \to R)$.

Then, we see a polynomial $f \in R[x]$ defines a corresponding map $\overline{f} \in \mathrm{Map}(R \to R)$ with $\overline{f}(a) = \mathrm{ev}_a(f)$ for all $a \in R$.

**Remark.** The map $f \mapsto \overline{f}$ need not be injective. See the example $f = x^5 - x$ and $g = 0$ in $\mathbb{F}_5$.

**Proposition 1.1.** If $R$ is an integral domain, then $R[x]$ is also an integral domain. Moreover, for nonzero polynomials $f, g \in R[x]$ we have $\deg(fg) = \deg(f) + \deg(g)$.

This prove is completely trivial hence it is omitted.

**Theorem 1.1.** If $F$ is a field, then $F[x]$ is a euclidean domain, a principal ideal domain, and a unique factorization domain.

*Proof.* Applying standard (euclidean) polynomial division with euclidean norm $\deg(f)$ for $f \in F[x]$ yields a euclidean domain (hence a PID and UFD). □

**Theorem 1.2.** If $R$ is a commutative ring then $R[x]$ is a principal ideal domain if and only if $R$ is a field.

*Proof.* One direction has already been shown.
Moreover if $R[x]$ is a PID, then $R$ is an integral domain. Hence, if $ab = a$ with $a, b \in R$, then $a = 0$ or $b = 0$, so $R$ is an integral domain as its a subring of $R[x]$.
Now, let $y \in R$be an arbitrary nonzero element. We wish to show $y$ a unit. Let $I = (y, x) \subseteq R[x]$. Then, since $R[x]$ is a Principal ideal domain, we have an $f \in I$ so that $(y, x) = (f)$. Note that we must have $f \neq 0$ as $x \neq 0$ and as $y \in (f)$ we see $y = hf$ for an $h \in R[x]$ which is nonzero. Since $R$ is an integral

domain, we see $\deg(f) = \deg(h) = 0$. Hence, $f$ is a nonzero constant $\alpha \in R$ . Hence, we have $x \in I = (\alpha)$ so $x = g\alpha$ for some $g \in [x]$. But, $R$ is an integral domain, so $1 = \deg(x) = \deg(\alpha) + \deg(g) = \deg(g)$. So, we have $g = ax + b$ for some nonzero $a \in R \setminus \{0\}$ and $b \in R$. Thus, $x = (ax + b)\alpha = (a\alpha x + b\alpha)$, hence $a\alpha = 1$ and $b\alpha = 0$ by the coefficient property of polynomial rings. Thus,

$$(\alpha) = (f) = I = (y, x) = R[x].$$

Hence, $1 \in (y, x) = R[x](y) + R[x](x)$. So, $1 = g_1 y + g_2 x$ for some $g_1, g_2 \in R[x]$. Hence letting $g_1 = g_{11} + g_{12}x$ and similairly $g_2 = g_{21} + g_{22}x$ for some $g_{11}, g_{12}, g_{21}, g_{22} \in R$, we see $1 = yg_{11}$. So, $y$ is a unit, hence $R$ is a field. □

**Corollary 1.** If $F$ is a field $F[x, y]$ is not a principal ideal domain.

*Proof.* $F[x, y] = (F[x])[y]$ and $F[x]$ is not a field (take $f = x$, there is no inverse), so $F[x, y]$ is not a principal ideal domain by applying the previous characterization. □

**Theorem 1.3.** If $F$ is a field with $f$ being a polynomial having $\deg(f) = n \geq 0$ in $F[x]$. If, $f(a) = 0$ for $a \in R$, then $(x - a) \mid f$. Moreover, $f$ has at most $n$ roots in $F$.

*Proof.* Since $f \neq 0$ and $f$ has a zero, we see $\deg(f) \geq 1$ . Hence, using polynomial long division yields $f = q(x - a) + r$ for some $q, r \in F[x]$ with $\deg(r) < \deg((x - a))$, hence $\deg(r) \leq 0$, that is $r$ is a constant polynomial.
We see $f(a) = r = 0$, hence $f = q(x - a)$, so $(-a) \mid f$. Letting $a_1, \ldots, a_n$ be distinct real zeros of $f$, then $(x - a_1) \mid f$ implying $f = f_1(x - a_1)$ with $\deg(f_1) = \deg(f) - 1$. Inducing on the roots $a_i$, we see that more than $n$ roots would imply $f = f_1 \cdot f_2 \cdot \ldots \cdot f_n \cdot f_{n+1} \cdot g$ where $g$ is the final polynomial obtained by dividing by $x - a_{n+1}$ and is of degree $\deg(g) = \deg(f) - (n + 1) = -1$ implying $g$ is the zero polynomial. But, we have $f = g \prod_{i=1}^{n+1}(x - a_i)$, so $f = 0$ $\lightning$. Hence there are at most $n$ zeroes. □