Polynomial Rings : Linear Algebra Notes

Satya Mandal

September 27, 2005

1 Section 1: Basics

Definition 1.1 *A nonempty set R is said to be a ring if the following are satisfied:*

1. *R has two binary operations, called addition (+) and multiplication.*
2. *R has an abelian group structure with respect to addition.*
3. *The additive identity is called zero and denoted by 0.*
4. *(Distributivity) For $x, y, z \in R$ we have $x(y+z) = xy + xz$ and $(y+z)x = yx + zx$.*
5. *We assume that there is a multiplicative identity denoted by $1 \neq 0$.*

Note the multiplication need not be commutative. So, it is possible that $xy \neq yx$. Also note that not all non-zero elements have an inverse. For example Let $R = M_{nn}(\mathbb{F})$ be the set of all $n \times n$ matrices ($n \geq 2$). Then R is a ring but multiplication is not commutative. Following are few more definitions:

Definition 1.2 Let R be a ring.

1. We say R is **commutative** if $xy = yx$ for all $x, y \in R$.
2. A commutative ring R is said to be an **integral domain** if

$$xy = 0 \Longrightarrow (x = 0 \quad or \quad y = 0).$$

3. Let A be another ring. A map $f : R \to A$ is said to be a ring homomorphism if for all $x, y \in R$ we have $f(x+y) = f(x) + f(y), f(xy) = f(x)f(y)$ and $f(1) = 1$.

4. For a ring R, an $R-$**algebra** is a ring A with together with a ring homomorphism $f : R \to A$.

Remark 1.1 Let $\mathbb{F}$ be a field and A be an $\mathbb{F}-$algebra. The textbook calls such an algebra as Linear Algebra. Note that A has a natural vector space structure.

Exercise 1.1 Let $\mathbb{F}$ be a field and $f : \mathbb{F} \to A$ be ring homomorphism. Then f is 1-1. *(This means that if A is an $\mathbb{F}-$algebra then $\mathbb{F} \subseteq A$.)*

Proof. It is enough to show that if $f(x) = 0$ then $x = 0$. (Are you sure that it is enough?) Assume $x \neq 0$ and $f(x) = 0$. We have $f(1) = 1$. So, $1 = f(xx^{-1}) = f(x)f(x^{-1})$. So, $f(x) \neq 0$.

2 Polynomials

We do not look at polynomials as functions. Polynomilas are formal expressions and (in algebra) they are manipulated formally.

Definition 2.1 Let $\mathbb{F}$ be a field and $\mathbb{N} = \{0, 1, 2, \ldots\}$ be the set of non-negative integers.

1. Let $\mathcal{F}$ denote the set of all functions $f : \mathbb{N} \to \mathbb{F}$. So,

$$\mathcal{F} = \{(a_0, a_1, a_2, \ldots) : a_i \in \mathbb{F}\}$$

   is the set of all infinite sequences in $\mathbb{F}$.

   Define addition and multiplication on $\mathcal{F}$ naturally (see the book).

   $\mathcal{F}$ is called the power series ring.

2. Let $X = (0, 1, 0, 0, \ldots) \in \mathcal{F}$. Then any element $f = (a_i) \in \mathcal{F}$ can be written as

$$f = \sum_{i=0}^{\infty} a_i X^i$$

with apprpriate meaning of infinite sum attached.

3. **Notation:** Usual notation for the power series ring is

$$\mathbb{F}[[X]] = \mathcal{F}.$$

Elements in $\mathbb{F}[[X]]$ are called **power series over** $\mathbb{F}$.

4. Let

$$\mathbb{F}[X] = \{f \in \mathbb{F}[[X]] : f = a_0 + a_1 X + \cdots + a_n X^n, a_i \in \mathbb{F}\}$$

Note that $\mathbb{F}[X]$ is a subring of $\mathbb{F}[[X]]$. We say that $\mathbb{F}[X]$ is the **polynomial ring over** $\mathbb{F}$.

5. **Importantly,** two polynomials f, g are equal if and only if coefficients of X^i are same for both f and g.

Theorem 2.1 Let $\mathbb{F}[X]$ be the polynomial ring over over a field $\mathbb{F}$.

1. Suppose $f, g, g_1, g_2 \in \mathbb{F}[X]$ and f is non zero. Then

$$(fg = 0 \Rightarrow g = 0) \quad \textit{and} \quad (fg_1 = fg_2 \Rightarrow g_1 = g_2).$$

2. $f \in \mathbb{F}[X]$ has an inverse in $\mathbb{F}[X]$ if and only if f is a nonzero scalar.

3 Section 4: Division and Ideals

Theorem 3.1 (Division Algorithm) *Let $\mathbb{F}$ is a field and $\mathbb{F}[X]$ be a polynomial ring over $\mathbb{F}$. Let $d \neq 0$ be a polynomial and $deg(D) = n$. Then for any $f \in \mathbb{F}[X]$, there are polynomials $q, r \in \mathbb{F}[X]$ such that*

$$f = qd + r \quad r = 0 \quad deg(r) < n.$$

In fact, q, r are UNIQUE for a given f.

Proof. Write a proof.

Corollary 3.1 *Let $\mathbb{F}$ is a field and $\mathbb{F}[X]$ be a polynomial ring over $\mathbb{F}$. Let f be a nonzero polynomial and $c \in \mathbb{F}$. Then $f(c) = 0$ if and only if $(X - c)$ divides f in $\mathbb{F}[X]$.*

Further, a polynomial f with $deg(f) = n$ has atmost n roots in $\mathbb{F}$.

Proof. ($\Leftarrow$): Obvious.
($\Rightarrow$): By division algorithm, we have $f = (X - C)Q + R$ where $R, Q \in \mathbb{F}[X]$ and either $R = 0$ or $deg(R) = 0$. We have $0 = f(c) = R(0) = R$. Therefore $f = (X - C)Q$

For the proof of the last assertion, use induction on n.

3.1 GCD

Definition 3.1 Let $\mathbb{F}$ be a filed and $\mathbb{F}[X]$ be the polynomial ring. Let $f_1, \ldots, f_r \in \mathbb{F}[X]$ be polynomials, not all zero. An element $d \in \mathbb{F}[X]$ is said to be a Greatest common divisor (gcd) if

1. $d|f_i \quad \forall \quad i = 1, \ldots, r$,
2. If there is an elment $d' \in \mathbb{F}[X]$ such that

$$d'|f_i \quad \forall \quad i = 1, \ldots, r$$

   then $d'|d$.

Lemma 3.1 *Let $\mathbb{F}$ be a filed and $\mathbb{F}[X]$ be the polynomial ring. Let $f_1, \ldots, f_r \in \mathbb{F}[X]$ be polynomials, not all zero. Suppose d_1 and d_2 are two GCDs of $f_1, \ldots, f_r$. Then*

$$d_1 = ud_2$$

for some unit $u \in \mathbb{F}$.

Further, if we assume that both d_1, d_2 are monic then $d_1 = d_2$. That means, monic GCD of $f_1, \ldots, f_r \in \mathbb{F}[X]$ is UNIQUE.

Proof. By property (2) of the definition, $d_1 = ud_2$ and $d_2 = vd_1$ for some $u, v \in \mathbb{F}[X]$. Hence $d_1 = uvd_1$. Since $d_1 \neq 0$, we have $uv = 1i$, so u is an unit.

Now, if d_1, d_2 are monic then comparing the coefficients of the top degree terms in the equation $d_1 = ud_2$ it follows that $u = 1$ and hence $d_1 = d_2$. This completes the proof.

Remarks. (1) Note that $\mathbb{Z}$ has only two unit, 1 and -1. When you computed GCD of integers, definition assumes that the GCD is positive. That is why GCD of integers is unique.

Definition 3.2 Let R be a (commutative) ring. A nonempty subset I of R is said to be an **ideal** of R if

1. $(x, y \in I) \Rightarrow (x + y \in I)$.
2. $(x \in R, \quad y \in I) \Rightarrow (xy \in I)$.

Example 3.1 Let R be a (commutative) ring. Let $f_1, \ldots, f_r \in R$. Let

$$I = \{x \in R : x = g_1 f_1 + \cdots + g_r f_r \quad for \quad g_i \in R\}.$$

Then I is an ideal of R. This ideal is sometime denoted by $(f_1, \ldots, f_r)$. Also

$$I = Rf_1 + \cdots + Rf_r.$$

Theorem 3.2 *Let $\mathbb{F}$ be a filed and $\mathbb{F}[X]$ be the polynomial ring. Let I be a non zero ideal of $\mathbb{F}[X]$. Then*

$$I = \mathbb{F}[X]d$$

for some $d \in \mathbb{F}[X]$. In fact, for any non-zero $d \in I$ with $deg(d)$ least, we have $I = \mathbb{F}[X]d$.

Proof. Let $k = min\{deg(f) : f \in I, \quad f \neq 0\}$. Pick $d \in I$ such that $d \neq 0$ and $deg(d) = k$. (Question: Why such a d exists?) Now claim $I = \mathbb{F}[X]d$.

Clearly, $I \supseteq \mathbb{F}[X]d$. Now, let $f \in I$. By division $f = qd + r$ with $r = 0$ or $deg(r) < k$. Note $r = f - qd \in I$. We prove $r = 0$. If $r \neq 0$, then $deg(r) < k$ would contradicts the minimality of k. So, $r = 0$ and $f = qd \in \mathbb{F}[X]d$. This completes the proof.

Theorem 3.3 *Let $\mathbb{F}$ be a filed and $\mathbb{F}[X]$ be the polynomial ring. Let $f_1, \ldots, f_r \in \mathbb{F}[X]$ be polynomials, not all zero.*

1. *Then $f_1, \ldots, f_r$ has a GCD. In fact, a GCD d of $f_1, \ldots, f_r$ is given by*
$$d = q_1 f_1 + \cdots + q_r f_r$$
for some $q_i \in \mathbb{F}[X]$.

2. *Two GCDs differ by a unit multiple.*

3. *A monic GCD is unique.*

Proof. Write
$$I = \mathbb{F}[X]f_1 + \cdots + \mathbb{F}[X]f_r$$

By above thorem, $I = \mathbb{F}[X]d$ for some $d \in \mathbb{F}[X]$. We calim that d is a GCD of $f_1, \ldots, f_r$. First note,
$$d = q_1 f_1 + \cdots + q_r f_r$$
for some $q_i \in \mathbb{F}[X]$.

Since $f_i \in I$, what have $d|f_i$. Now let $d' \in I$ be such that $d'|f_i$, for $i = 1, \ldots, r$. We need to prove that $d'|d$. This follows from the above equation. This completes that proof that GCD exist. We have alrady seen (2) and (3) before.

4 Prime Factorization

Definition 4.1 Let $\mathbb{F}[X]$ be a the polynomial ring over a field $\mathbb{F}$.

1. An element $f \in \mathbb{F}[X]$ is said to be a an **reducible over** $\mathbb{F}$ if $f = gh$ for some non-unit $g, h \in \mathbb{F}[X]$ (equivalently, $deg(g) > 0$ and $deg(h) > 0$.)

2. $f \in \mathbb{F}[X]$ is said to be **irredubible over** $\mathbb{F}$ if it is not reducible.

3. A non-scalar irreducible element $f \in \mathbb{F}[X]$ over $\mathbb{F}$ is called a **prime** in $\mathbb{F}[X]$.

Lemma 4.1 Let R be an integral domain. For non-zero $f, g \in R$, $Rf = Rg$ if and only if $f = ug$ for some unit in R.

Proof. Easy.

Lemma 4.2 Let $R = \mathbb{F}[X]$ be the polynomial ring over a field $\mathbb{F}$. Let $p \in R$ be a prime element and $f \in R$. Then

$$(Rf + Rp = R) \quad \Longleftrightarrow \quad (p \textit{ does not divide } f.)$$

Proof. ($\Rightarrow$): We prove by contradiction. Assume that $p \mid f$. Then $f = dp$ for some $d \in R$. Hence $Rf + Rp = Rdp + Rp = Rp \neq R$. So, this part of the proof is complete.
($\Leftarrow$): Assume p does not divide f. By Theorem 3.2, we have $Rf + Rp = Rd$ for some $d \in R$. Therefore $f = ud$ and $p = vd$ for some $u, v \in R$. Claim d is a unit.

If not, since p is prime, v is an unit. Hence $f = ud = uv^{-1}p$. That means, $p \mid f$. This will be a contradiction. Therefore the claim is proved and d is a unit. Hence $Rf + Rp = Rd = R$ The proof is complete.

Theorem 4.1 *Let $R = \mathbb{F}[X]$ be the polynomial ring over a field $\mathbb{F}$. Let $p \in R$ be a prime element and $f, g \in R$. Then*

$$p \mid fg \quad \Rightarrow \quad \textit{either} \quad p \mid f \quad \textit{or} \quad p \mid g.$$

Proof. Assume $p \mid fg$ and p does not divide f. We will prove that $p \mid g$.

We have $fg = pw$ for some $w \in R$. Also by above lemma 4.2, $Rf + Rp = R$. Therefore, $1 = xf + yp$ for some $x, y \in R$. Hence $g = xfg + yp = xwp + yp$. This completes the proof.

Corollary 4.1 *Let $R = \mathbb{F}[X]$ be the polynomial ring over a field $\mathbb{F}$. Let $p \in R$ be a prime element and $f_1, f_2, \ldots, f_r \in R$. Then*

$$p \mid f_1 f_2 \cdots f_r \quad \Longrightarrow \quad p \mid f_i$$

for some $i = 1, \ldots, r$.

Proof. Use induction and the above thoerem.

Theorem 4.2 (Unique Factorization) *Let $R = \mathbb{F}[X]$ be the polynomial ring over a field $\mathbb{F}$. Let $f \in R$ be a nonzero element. Then*

$$f = up_1 p_2 \cdots p_k$$

where $u \in \mathbb{F}$ is a unit and $p_1, \ldots, p_k$ are monic prime elements. In fact, this factorizton is unique, except for order.

Proof. First we prove that factorization, as above, of f is possible. Let $deg(f) = n$. we will use induction on n.
Case $n = 0$: If $n = 0$ then f is an unit and we are done.
Case $n = 1$: In this case, $f = uX + v$ with $u, v \in \mathbb{F}$ and $u \neq 0$. Write $p = X + v/u$. The p is prime and $f = up$.
Case $n > 1$: If f is prime, then write $f = uX^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$, with $u, a_i \in \mathbb{F}$ and $u \neq 0$. Write $p = f/u$. The p is monic prime and $f = up$.

Now, if f is not a prime, then $f = gh$ with $deg(g) < n$ and $deg(h) < n$. By induction, g and h have factorization as desired. The product of these two factorizations will give a desired factorization of f.

So, the proof of existance of the factorization is complete.

Now we will prove the uniqueness of the factorization. Suppose

$$f = up_1 p_2 \cdots p_k = vq_1 q_2 \cdots q_m$$

where u, v are units and p_i, q_j are monic primes.

Assume $deg(f) = n$. By comparing coefficients of X^n we get $u = v$. Therefore, we have

$$g = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$$

where $g = f/u$ is monic.

Now $p_1 \mid q_1 q_2 \cdots q_m$. By Corollary 4.1, $p_1 \mid q_j$ for some j. we may assume $j = 1$ and $p_1 \mid q_1$. Since both p_1, q_1 are monic primes, we have $p_1 = q_1$.

Hence it follows

$$p_2 \cdots p_k = q_2 \cdots q_m.$$

Therefore, by induction, $k = m$ and $p_i = q_i$ upto order. This completes the proof.