Polynomial rings

1. POLYNOMIALS

Throughout this section, $R$ is a commutative ring with identity

**Definition 1.** A polynomial over $R$ in indeterminate $x$ is an expression of the form

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

where $a_i \in R$. The set of such polynomials is denoted $R[x]$.

The elements $a_i$ are the coefficients of $f$. The degree of $f$ is the largest $m$ such that $0 \neq a_m$ if such an $m$ exists. We write $\deg(f) = m$ and say $a_m$ is the leading coefficient. Otherwise $f = 0$ and we set $\deg(f) = -\infty$. A nonzero polynomial with leading coefficient 1 is called monic.

Let $p(x), q(x) \in R[x]$ be nonzero polynomials with degrees $n$ and $m$, respectively. Write

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n$$

$$q(x) = b_0 + b_1 x + \cdots + b_m x^m.$$  

The polynomials $p(x)$ and $q(x)$ are equal ($p(x) = q(x)$) if and only if $n = m$ and $a_i = b_i$ for all $i$.

We can define two binary operations, addition and multiplication, on $R[x]$. Suppose $n \geq m$ and set $b_i = 0$ for $i > m$. Then

$$p(x) + q(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n.$$ 

This is similar if $m > n$. Now

$$p(x)q(x) = c_0 + c_1 x + \cdots + c_{m+n} x^{m+n},$$

where

$$c_i = \sum_{k=0}^{i} a_0 b_i + a_1 b_{i-1} + \cdots + a_{i-1} b_1 + a_i b_0.$$

**Theorem 1.** Let $R$ be a commutative ring with identity. Then $R[x]$ is a commutative ring with identity.

**Proof.** Above we showed that addition and multiplication are binary operations. It is easy to check that $(R[x], +)$ is an abelian group where the zero polynomial is the (additive) identity. The multiplicative identity is the constant polynomial 1. Associativity of multiplication and the distributive property are easy (albeit annoying) proofs. The details are left as an exercise.  

These notes are derived primarily from *Abstract Algebra, Theory and Applications* by Thomas Judson (16ed). Most of this material is drawn from Chapter 17. Last Updated: November 20, 2019
**Example.** Suppose \( p(x) = 3 + 2x^3 \) and \( q(x) = 2 - x^2 + 4x^4 \) are polynomials in \( \mathbb{Z}[x] \). Note that \( \deg(p(x)) = 3 \) and \( \deg(q(x)) = 4 \). Then

\[
p(x) + q(x) = (3 + 2) + (0 + 0)x + (0 - 1)x^2 + (2 + 0)x^3 + (0 + 4)x^4 = 5 - x^2 + 2x^3 + 4x^4
\]

and

\[
p(x)q(x) = (3 + 2x^3)(2 - x^2 + 4x^4) = 6 - 3x^2 + 4x^3 + 12x^4 - 2x^5 + 8x^7.
\]

**Example.** Let \( p(x) = 3 + 3x^3 \) and \( q(x) = 4 + 4x^2 + 4x^4 \) be polynomials in \( \mathbb{Z}_{12}[x] \). Then \( p(x) + q(x) = 7 + 4x^2 + 3x^3 + 4x^4 \) and \( p(x)q(x) = 0 \).

**Proposition 2.** If \( R \) be an integral domain, then \( R[x] \) is an integral domain.

**Proof.** Let \( p(x), q(x) \in R[x] \) be nonzero polynomials with degrees \( n \) and \( m \), respectively. Write

\[
p(x) = a_0 + a_1x + \cdots + a_nx^n
\]
\[
q(x) = b_0 + b_1x + \cdots + b_mx^m.
\]

Then the leading term of \( p(x)q(x) \) is \( a_nb_mx^{n+m} \). By hypothesis, \( a_n, b_m \neq 0 \) and because \( R \) is an integral domain, \( a_nb_m \neq 0 \) so \( p(x)q(x) \neq 0 \).

**Remark.** What we actually proved in the last proposition was that for an integral domain \( R \),

\[\deg(p(x), q(x)) = \deg(p(x)) + \deg(q(x)),\]

for any polynomials \( p(x), q(x) \in R[x] \). This justifies why we set \( \deg(0) = -\infty \).

So far we’ve discussed polynomials in one variable, but it is relatively straightforward, albeit very tedious, to define polynomials in two or more variables. By the above theorem, if \( R \) is a commutative ring with identity then so is \( R[x] \). If \( y \) is another indeterminate, then it makes sense to define \( (R[x])[y] \). One could then show that this ring is isomorphic to \( (R[y])[x] \). Both of these rings will be identified with the ring \( R[x, y] \) and call this the ring of polynomials in two indeterminates \( x \) and \( y \) with coefficients in \( R \). Similarly (or inductively), one can then define the ring of polynomials in \( n \) indeterminates with coefficients in \( R \), denoted \( R[x_1, \ldots, x_n] \).

**Theorem 3.** Let \( S \) be a commutative ring with identity and \( R \) a subring of \( S \) containing 1. Let \( \alpha \in S \). If \( p(x) = a_0 + a_1x + \cdots + a_nx^n \), then we define \( p(\alpha) \) to be

\[
p(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n \in S.
\]

Then there is a ring homomorphism \( R[x] \to S \) given by \( p(x) \mapsto p(\alpha) \).

**Definition 2.** The map in the previous theorem is called the evaluation homomorphism at \( \alpha \). We say \( \alpha \in R \) is a root (or zero) of \( p(x) \in R[x] \) if \( \phi_\alpha(p(x)) = 0 \).
2. Divisibility

We will now prove a version of the division algorithm for polynomials. This will be applied to determine when polynomials are irreducible over certain rings.

**Theorem 4.** Let $F$ be a field and $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. Then there exist unique polynomials $f(x), r(x) \in F(x)$ such that

$$f(x) = g(x)q(x) + r(x),$$

where $\deg r(x) < \deg g(x)$.

**Proof.** For simplicity throughout we will write $f = f(x), g = g(x)$, etc. Set $\deg f = n$ and $\deg g = m$. If $n < m$, then let $q = 0$ and $r = f$. Note that this may happen if $f = 0$.

Now suppose $m \leq n$. Write

$$f = a_0 + a_1x + \cdots + a_nx^n$$

$$g = b_0 + b_1x + \cdots + b_mx^m.$$  

Because $b_m \neq 0$ and $F$ is a field, $b_m^{-1}$ exists.

If $n = 0$, then $m = 0$ so $f = c_0$ and $g = b_0$. Set $q = a_0b_0^{-1}$ and $r = 0$.

We proceed inductively. That is, assume the division algorithm holds when $\deg f < n$. Note that $f - a_n b_m^{-1} x^{n-m} g$ has degree strictly less than $n$. Hence, there exists $q_0, r$ such that $f - a_n b_m^{-1} x^{n-m} g = q_0 g + r$ with $\deg r < \deg g$. This implies that

$$f = (q_0 + a_n b_m^{-1} x^{n-m}) g + r.$$  

Setting $q = q_0 + a_n b_m^{-1} x^{n-m}$ completes the existence part of the proof.

For uniqueness, assume there exists $q, q', r, r' \in F[x]$ such that $f = qg + r = q'g + r'$ with $\deg r, \deg r' < \deg g$. Then $g(q - q') = r' - r$. If $q \neq q'$, then because $g \neq 0$ we have

$$\deg(r' - r) = \deg(g(q - q')) \geq \deg g.$$  

This is a contradiction since both $r'$ and $r$ have degrees less than $\deg g$. Thus, $q = q'$ and so $r = r'$.

**Corollary 5.** Let $F$ be a field. An element $\alpha \in F$ is a root of $p(x) \in F[x]$ if and only if $(x - \alpha)$ divides (is a factor of) $p(x)$.

**Proof.** By the division algorithm, $p(x) = (x - \alpha)q(x) + r(x)$ for some $q(x), r(x) \in F[x]$ with $\deg r(x) < \deg(x - \alpha) = 1$. Applying the evaluation homomorphism we get $p(\alpha) = (\alpha - \alpha)q(\alpha) + r(\alpha) = r(\alpha)$. If $x - \alpha$ divides $p(x)$, then $r(x) = 0$ so $p(\alpha) = 0$ and $\alpha$ is a root of $p(x)$. Conversely, if $\alpha$ is a root, then $r(\alpha) = 0$. But $\deg r < 1$ and since $r(x)$ cannot be a nonzero constant, then $r(x) = 0$.  

\[\square\]
Corollary 6. Let $F$ be a field. A nonzero polynomial $p(x) \in F[x]$ of degree $n$ can have at most $n$ distinct roots.

Proof. First note that a polynomial of degree 0 has no roots. Let $p(x) \in F[x]$ have degree $n$. If $n = 1$, then $p(x)$ has 1 root. We proceed by induction on $\deg p(x)$. Suppose all polynomials of degree $m$, $m \geq 1$, have at most $m$ distinct roots. Let $\deg p(x) = m + 1$ and let $\alpha$ be a root of $p(x)$. By the previous corollary, $p(x) = (x - \alpha)q(x)$ for some $q(x)$ with $\deg q(x) = m$. Thus, $m$ has at most $m$ distinct roots and so $p(x)$ has at most $m + 1$ distinct roots. □

The next proof is very similar to the corresponding result for $\mathbb{Z}$.

Corollary 7. Let $F$ be a field. Every ideal in $F[x]$ is principal.

Proof. Let $I$ be a nonzero ideal in $F[x]$. Set $S = \{\deg p(x) : p(x) \in I, p(x) \geq 0\}$. Since $I \neq 0$, then $S \neq \emptyset$ and $S \subset \mathbb{N}$. Thus, by the Well-Ordering Principal, $S$ has a least element, $d$. Let $g(x) \in I$ be a polynomial of degree $d$. We claim $I = \langle g(x) \rangle$. It is clear that $\langle g(x) \rangle \subset I$ and so it is left only to prove the reverse inclusion.

Let $f(x) \in I$. If $\deg f(x) = d$, then either $f(x) = ag(x)$ for some $a \in F$ or else $\deg(f(x) - g(x)) < d$, a contradiction since $f(x) - g(x) \in I$. Now assume $\deg f(x) > d$. By the division algorithm, $f(x) = g(x)q(x) + r(x)$ for some $q(x), r(x) \in I$ with $\deg r(x) < \deg g(x)$. But then $r(x) = f(x) - g(x)q(x) \in I$. If $\deg r(x) \geq 0$, then this contradicts the minimality of $d$. Thus, $r(x) = 0$ and $f(x) \in \langle g(x) \rangle$. □

Warning. The above result does not hold for $F[x, y]$. In particular, the ideal $\langle x, y \rangle$ is not principal.
3. Irreducible Polynomials

**Definition 3.** Let $F$ be a field. A nonconstant polynomial $f(x) \in F[x]$ is irreducible over $F$ if $f(x)$ cannot be written as a product of two polynomials $g(x), h(x) \in F[x]$ with $\deg g(x), \deg h(x) < \deg f(x)$.

**Example.**
1. $x^2 - 2$ is irreducible over $\mathbb{Q}$.
2. $x^2 + 1$ is irreducible over $\mathbb{R}$.
3. $p(x) = x^3 + x^2 + 2$ is irreducible over $\mathbb{Z}_3$. To see this, just note that $p(0) = 2$, $p(1) = 1$, and $p(2) = 2$, so $p(x)$ does not have a root in $\mathbb{Z}_3$.

**Lemma 8.** Let $p(x) \in \mathbb{Q}[x]$. Then

$$p(x) = \frac{r}{s}(a_0 + a_1x + \cdots + a_nx^n),$$

where $r, s, a_0, \ldots, a_n \in \mathbb{Z}$, the $a_i$ relatively prime, and $r, s$ relatively prime.

**Proof.** Write, $a_i = b_i/c_i$ with $b_i, c_i \in \mathbb{Z}$. Then

$$p(x) = \frac{1}{c_0 \cdots c_n} (d_0 + d_1x + \cdots + d_nx^n),$$

where the $d_i$ are integers. Set $d = \gcd\{d_0, \ldots, d_n\}$. Set $a_i = d_i d^{-1}$ and let $\frac{r}{s} = \frac{d}{c_0 \cdots c_n}$ written in lowest terms. The result follows.

**Theorem 9** (Gauss’ Lemma). If a non-constant monic polynomial $p(x) \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Z}$, then it is irreducible over $\mathbb{Q}$.

**Proof.** We will prove the contrapositive. Let $p(x) \in \mathbb{Z}[x]$ be a non-constant polynomial and suppose it factors over $\mathbb{Q}$. We will show that it factors over $\mathbb{Z}$.

Write $p(x) = \alpha(x)\beta(x)$ for some monic polynomials $\alpha(x), \beta(x) \in \mathbb{Q}[x]$ with $\deg \alpha(x), \deg \beta(x) < \deg p(x)$. By the previous lemma,

$$\alpha(x) = \frac{c_1}{d_1} (a_0 + a_1x + \cdots + a_mx^m) = \frac{c_1}{d_1} \alpha_1(x) \quad (a_m \neq 0),$$

$$\beta(x) = \frac{c_2}{d_2} (b_0 + b_1x + \cdots + b_nx^n) = \frac{c_2}{d_2} \beta_1(x) \quad (b_n \neq 0),$$

where the $a_i$ are relatively prime and the $b_i$ are relatively prime. Then

$$p(x) = \frac{c_1 c_2}{d_1 d_2} \alpha_1(x) \beta_1(x).$$

Set $\frac{c}{d} = \frac{c_1 c_2}{d_1 d_2}$ expressed in lowest terms. Thus, $dp(x) = c\alpha_1(x)\beta_1(x)$. We now consider several cases.

**Case 1:** $(d = 1)$ Because $p(x)$ is monic, then $ca_mb_n = 1$. As all three factors are integers, so then $c, a_m, b_n \in \{-1, 1\}$. Suppose $c = a_m = b_n = 1$, then $p(x) = \alpha_1(x)\beta_1(x)$ and this proves the claim. If $c = 1$ and $a_m = b_n = -1$, then $p(x) = (-\alpha_1(x))(-\beta_1(x))$. The remaining cases are left as an exercise.
Case 2: \((d \neq 1)\) Since \(\gcd(c, d) = 1\), there exists a prime \(p\) such that \(p \mid d\) and \(p \nmid c\). The coefficients of \(\alpha_1(x)\) are relatively prime and so there exists a coefficient \(a_i\) of \(\alpha_1(x)\) such that \(p \nmid a_i\). Similarly, there exists a coefficient \(b_j\) of \(\beta_1(x)\) such that \(p \nmid b_j\). Let \(\alpha'_1(x)\) and \(\beta'_1(x)\) be the images of \(\alpha_1(x)\) and \(\beta_1(x)\) in \(\mathbb{Z}_p[x]\). Since \(p \mid d\), \(\alpha'_1(x)\beta'_1(x) = 0\). But this is impossible since neither \(\alpha'_1(x)\) or \(\beta'_1(x)\) are the zero polynomial and \(\mathbb{Z}_p[x]\) is an integral domain. Therefore, \(d = 1\). \(\square\)

Corollary 10. Let \(p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0\) be a polynomial with coefficients in \(\mathbb{Z}\) and \(a_0 \neq 0\). If \(p(x)\) has a zero in \(\mathbb{Q}\), then \(p(x)\) also has a zero in \(\mathbb{Z}\). Furthermore, \(\alpha\) divides \(a_0\).

Proof. Let \(p(x)\) have a zero \(a \in \mathbb{Q}\). Then \(p(x)\) has a linear factor \(x - a \in \mathbb{Q}[x]\). By Gauss’ Lemma, \(p(x)\) has a factorization with a linear factor in \(\mathbb{Z}[x]\). Hence, for some \(\alpha \in \mathbb{Z}\).

\[
p(x) = (x - \alpha)(x^{n-1} + \cdots - a_0/\alpha).
\]

Thus, \(a_0/\alpha \in \mathbb{Z}\) and so \(\alpha \mid a_0\). \(\square\)

Example. Let \(p(x) = x^4 - 2x^3 + x + 1\). We will show that \(p(x)\) is irreducible over \(\mathbb{Q}\).

Case 1: Suppose \(p(x)\) has a linear factor in \(\mathbb{Q}[x]\), so \(p(x) = (x - a)q(x)\) for some \(q(x) \in \mathbb{Q}[x]\). Then \(p(x)\) has a zero in \(\mathbb{Z}\) (by Gauss’ Lemma) and \(\alpha \mid 1\) (by the corollary), so \(\alpha = \pm 1\). But \(p(1) = 1\) and \(p(-1) = 3\), so \(p(x)\) has no linear factors.

Case 2: Suppose \(p(x)\) is the product of two (irreducible) quadratic factors. By Gauss’s Lemma, \(p(x)\) factors over \(\mathbb{Z}[x]\) and so

\[
p(x) = (x^2 + ax + b)(x^2 + cx + d)
\]

\[
x^4 - 2x^3 + x + 1 = x^4 + (a + c)x^3 + (b + d + ac)x^2 + (ad + bc)x + bd.
\]

where \(a, b, c, d \in \mathbb{Z}\). Thus, \(bd = 1\) so \(b = d = \pm 1\). Then

\[
1 = ad + bc = (a + c)b = -2b.
\]

This implies \(1 = \pm 2\), a contradiction. Hence, \(p(x)\) is irreducible.

The following actually requires a stronger version of Gauss’ Lemma that we will not prove here.

Theorem 11 (Eisenstein’s Criterion). Let \(p\) be a prime and suppose that

\[
f(x) = a_nx^n + \cdots + a_0 \in \mathbb{Z}[x].
\]

If \(p \mid a_i\) for \(i = 0, 1, \ldots, n - 1\), but \(p \nmid a_n\) and \(p^2 \nmid a_0\), then \(f(x)\) is irreducible over \(\mathbb{Q}\).

Proof. If suffices by Gauss’ Lemma to prove that \(f(x)\) does not factor over \(\mathbb{Z}[x]\). Let

\[
f(x) = (b_r x^r + \cdots + b_0)(c_s x^s + \cdots + c_0)
\]

where \(r, s \geq 2\). Since \(p \mid a_i\) for \(i = 0, 1, \ldots, n - 1\), but \(p \nmid a_n\) and \(p^2 \nmid a_0\), then \(f(x)\) is irreducible over \(\mathbb{Q}\).
be such a factorization with \( b_r, c_s \neq 0 \) and \( r, s < n \). Since \( p^2 \nmid a_0 = b_0c_0 \), either \( b_0 \) or \( c_0 \) is not divisible by \( p \). Suppose \( p \nmid b_0 \) and \( p \mid c_0 \) (the other case is similar). Since \( p \nmid a_n \) and \( a_n = b_r c_s \), neither \( b_r \) nor \( c_s \) is divisible by \( p \). Let \( m \) be the smallest value of \( k \) such that \( p \nmid c_k \). Then

\[
a_m = b_0 c_m + b_1 c_{m-1} + \cdots + b_m c_0
\]

is not divisible by \( p \) since all but one of the terms \((b_0 c_m)\) is divisible by \( p \). Therefore, \( m = n \) since \( a_i \) is divisible by \( p \) for \( m < n \). Hence, \( f(x) \) cannot be factored and is therefore irreducible. \( \square \)

**Example.** Let \( f(x) = 16x^5 - 9x^4 + 3x^2 + 6x - 21 \) and set \( p = 3 \). Then clearly \( p \) divides all coefficients except for that of \( x^5 \) and \( p^2 \nmid 21 \). Thus, \( f(x) \) is irreducible over \( \mathbb{Q} \) by Eisenstein’s Criterion.