Math 403 Chapter 16: Polynomial Rings

1. **Introduction:** We've seen many examples of polynomial rings like $\mathbb{Z}[x]$ and $\mathbb{R}[x]$. The job of this chapter is to formalize these and look at some overall properties.

2. **Basic Construction**

   (a) **Definition:** Let R be a commutative ring. Define:

   $$R[x] = \left\{ r_n x^n + r_{n-1}x^{n-1} + ... + r_1 x + r_0 \,|\, r_i \in R \right\}$$

   The letter x here can be thought of a variable or just as a placeholder. Either way the familiar structure allows us to add, subtract and multiply these as we do traditional polynomials even if the ring were some strange abstract entity.

   (b) **Theorem/Definition:** If R is a ring then so is $R[x]$, called the *ring of polynomials over (with coefficients in)* R, under familiar addition and multiplication methods derived from polynomials noting that the coefficients inherit their behavior from the original ring.
   Proof: Straightfoward. $\mathcal{QED}$

   For example in $Z_3[x]$ we would do something like:

   $$\begin{aligned}(2x^2+x+1)(x+2) &= (2x^2+x+1)(x) + (2x^2+x+1)(2) \\ &= 2x^3 + x^2 + x + 4x^2 + 2x + 2 \\ &= 2x^3 + 2x^2 + 2\end{aligned}$$

3. **Properties:**

   (a) **Theorem:** If D is an integral domain then so is $D[x]$.
   Proof: We need to show that $D[x]$ is commutative with unity and no zero-divisors. The unity is the unity from D and commutativity follows from the commutativity of D and the definition of multiplication in $D[x]$. To see that $D[x]$ has no zero-divisors take $p(x) = r_n x^n + ...$ and $q(x) = s_m x^m + ...$ in $D[x]$ with $r_n, s_m \neq 0$ and suppose that $p(x)q(x) = 0$. Since $p(x)q(x) = r_n s_m x^{n+m} + ...$ we then must have $r_n s_m = 0$ implying either $r_n = 0$ or $s_m = 0$, a contradiction. $\mathcal{QED}$

   Note: It follows also that in $D[x]$ when polynomials are multiplied the degrees are added. This is not true if D is not an integral domain, for example in $\mathbb{Z}_6[x]$ we have $(3x+2)(4x+5) = 12x^2 + 23x + 10 = 5x + 4$.

   (b) **Theorem (The Division Algorithm for $F[x]$):** Let F be a field and let $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. Then there exist unique $q(x), r(x) \in F[x]$ with $0 \leq \deg(r(x)) < \deg(g(x))$ and $f(x) = q(x)g(x) + r(x)$.
   Proof: The basic idea is to formalize the process of long division in an inductive sense. We omit the details, they're not much fun. $\mathcal{QED}$

   Note: This division is essentially long division of polynomials but can be confusing because the values are chosen from the field R which might not be familar:

   Example: In $\mathbb{Z}_3$ we can divide $2x^2+1$ into $x^4 + 2x^3 + 2x + 1$:

   $$\begin{array}{r|ccccc}
    & 2x^2 & +x & +2 & & \\ \hline
   2x^2+1 & x^4 & +2x^3 & +0x^2 & +2x & +1 \\
    & x^4 & & +2x^2 & & \\ \hline
    & & 2x^3 & +x^2 & +2x & +1 \\
    & & 2x^3 & & +x & \\ \hline
    & & & x^2 & +x & +1 \\
    & & & x^2 & & +2 \\ \hline
    & & & & x & +2
   \end{array}$$

   Thus we have $x^4 + 2x^3 + 2x + 1 = (2x^2+x+2)(2x^2+1) + (x+2)$.

(c) **Corollary (The Remainder Theorem):** Let F be a field, $a \in F$ and $f(x) \in F[x]$. Then $f(a)$ is the remainder when $f(x)$ is divided by $x - a$.
Proof: By the Division Algorithm we have $f(x) = q(x)(x-a) + b$ and then $f(a) = q(a)(a-a) + b = b$. $\mathcal{QED}$

(d) **Corollary (The Factor Theorem):** Let F be a field, $a \in F$ and $f(x) \in F[x]$. Then a is a zero/root of $f(x)$ iff $x - a$ is a factor of $f(x)$.
Proof: Well, a is a zero/root of $f(x)$ iff $f(a) = 0$ but by the previous colloary $f(a)$ is the remainder when $f(x)$ is divided by $x - a$. It follows that a is a zero/root of $f(x)$ iff $f(x) = q(x)(x-a) + 0$ and the result follows. $\mathcal{QED}$
Definition: A factor of the form $ax + b$ is a *linear factor*. Since $ax + b = a(x + a^{-1}b)$ we know that roots correspond to linear factors.

(e) **Theorem (Counting Zeros/Roots):** A polynomial of degree n over a field F has at most n zeros/roots, counting multiplicity.
Note: If R is not a field then this may not be true, for example in $\mathbb{Z}_6[x]$ the polynomial $f(x) = x^2 + x$ has four roots since $f(0) = f(2) = f(3) = f(5) = 0$.
Proof: By the previous corollary we show that the polynomial has at most n linear factors. We proceed by induction on n. If $n = 1$ then the polynomial has degree $n = 1$ and hence has the form $p(x) = ax + b = a(x + a^{-1}b)$ for $a, b \in F$ and hence has a single linear factor. Suppose the statement is true for some $k \geq 1$ and let $p(x)$ have degree $k+1$. If $p(x)$ has no linear factors then we are done, otherwise let $x - a$ be one such linear factor and so $p(x) = (x-a)q(x)$ where $\deg(q(x)) = k$. By the induction hypothesis $q(x)$ has k or fewer linear factors and hence $p(x)$ has $k+1$ or fewer. $\mathcal{QED}$

4. **Principal Ideal Domains**

(a) **Definition:** A *principal ideal domain (PID)* is an integral domain R in which every ideal has the form $\langle a \rangle$ for some $a \in R$. Recall that $\langle a \rangle = \{ra \mid r \in R\}$.

(b) **Theorem:** If F is a field then $F[x]$ is a PID.
Proof: We know $F[x]$ is an integral domain since F is an integral domain. Let I be an ideal of $F[x]$.

- If $I = \{0\}$ then $I = \langle 0 \rangle$ and we are done.
- If $I \neq \{0\}$ let $g(x)$ be a non-zero polynomial of minimal degree in I (which exists by well-ordering). If $g(x)$ is constant then $g(x) = \alpha \in F$ and then $I = F = \langle \alpha \rangle$ because for any $r \in F$ we have $r = r\alpha^{-1}\alpha \in \langle \alpha \rangle$. Suppose then that $g(x)$ is not constant, we claim $I = \langle g(x) \rangle$. Since $g(x) \in I$ we have $\langle g(x) \rangle \subseteq I$. We claim $I \subseteq \langle g(x) \rangle$. Let $f(x) \in I$. By the Division Algorithm write $f(x) = q(x)g(x) + r(x)$ with $0 \leq \deg(r(x)) < \deg(g(x))$. Since $r(x) = f(x) - q(x)g(x)$ we have $r(x) \in I$ and the fact that $g(x)$ is a nonzero polynomial of minimal degree implies that $r(x) = 0$ and so $f(x) = q(x)g(x)$ and so $f(x) \in \langle g(x) \rangle$.

$\mathcal{QED}$

(c) **Corollary:** Let F be a field and let I be a nonzero ideal of $F[x]$. Let $g(x) \in F[x]$. Then $I = \langle g(x) \rangle$ iff $g(x)$ is a nonzero polynomial of minimum degree in I.
Proof: This is also established by the proof above. $\mathcal{QED}$

(d) **Note:** If R is not a field then this is not the case, for example in $\mathbb{Z}[x]$ the ideal $\langle x, 2 \rangle$ is not principal. This isn't simply because we've generated it by two polynomials but rather that it cannot be genereted by one. There is no $p(x) \in \mathbb{Z}[x]$ such that $\langle p(x) \rangle = \langle x, 2 \rangle$. Can you show this?