Math 476 - Abstract Algebra 1
Day 33 Group Assignment **Name:**____________________________________

Polynomial Rings

Definition 11.2 Let R be a commutative ring. A **polynomial in x over R** is an expression of the form: $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x^1 + a_0x^0$, where n is a non-negative integer, and $a_n, a_{n-1}, \cdots, a_2, a_1, a_0$ are elements of R. The **set of all polynomials over the ring R** will be denoted by $R[x]$. We will generally assume that $a_n \neq 0$.

- The symbol x is called an **indeterminate**. It is to be regarded as a formal symbol and not as an element of the ring R. In effect, the symbols $x^0, x^1, x^2, \cdots, x^n$ serve as placeholders alongside the ring elements $a_0, a_1, \cdots, a_n$.
- The expressions a_kx^k are called the **terms of the polynomial**. The elements $a_0, a_1, \cdots, a_n$ in the ring R are called the **coefficients** of the polynomial $p(x)$. We call a_k the coefficient of x^k in the representation of $p(x)$.
- When working with a polynomial, instead of writing x^1, we simply write x. In addition, we usually do not write x^0 and we will write a_0x^0 simply as a_0 (does this make sense when R does not have an element 1_R?). Using these conventions, we can write $p(x)$ in the form $p(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x + a_0$, where n is a non-negative integer, $a_n, a_{n-1}, \cdots, a_2, a_1, a_0$ are elements of R, and $a_n \neq 0$.
- We will usually omit any term having a zero coefficient for the representation of a polynomial. If the ring has an identity, we will write a term of the form 1_Rx^k simply as x^k. We will also often write terms of the form $(-a_k)x^k$ as $-a_kx^k$. For example, in $R[x]$, instead of writing $f(x) = 3x^4 + 1x^3 + (-7)x^2 + 0x + 5$, we will write $f(x) = 3x^4 + x^3 - 7x^2 + 5$.
- The coefficient a_0 is called the **constant term** of the polynomial $p(x)$. A polynomial of the form $p(x) = a$ where $a \in R$ is called a **constant polynomial**.
- The coefficient a_n is called the **leading coefficient** of the polynomial $p(x)$. If the ring R has an identity and the leading coefficient a_n is equal to 1_R, the polynomial is called a **monic polynomial**.
- The non-negative integer n is called the **degree** of the polynomial $p(x)$, and we write $\deg(p(x)) = n$.
- We will use 0 to denote the polynomial in $R[x]$ having all of its coefficients equal to zero. This polynomial is called the **zero polynomial**. Since it does not have a leading coefficient, the degree of the zero polynomial is undefined.
- Two polynomials $p(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x^1 + a_0x^0$ and $q(x) = b_nx^n + b_{n-1}x^{n-1} + \cdots + b_2x^2 + b_1x^1 + b_0x^0$ are considered to be **equal polynomials** if both are the zero polynomial, or if both have the same degree and all pairs of corresponding coefficients are equal.
- When we write a polynomial in the form $p(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x + a_0$, we say that we have written the polynomial in **descending powers of x**. Similarly, a polynomial in the form $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + a_nx^n$ is said to be written in **ascending powers of x**.
- We may take the time to define polynomial addition and polynomial multiplication more formally later, but for now, it will suffice to say that we will carry out these operations in a manner similar to what you learned in your previous algebra courses (combine like terms when adding; expand, simplify exponents, and combine like terms when multiplying).

1. Let R be a commutative ring. Let $p(x) = a_2x^2 + a_1x + a_0$, $q(x) = b_2x^2 + b_1x + b_0$, and $r(x) = c_1x + c_0$.

   (a) Let $z(x) = 0$ be the zero polynomial in $R[x]$. Verify that $z(x)$ is an additive identity in $R[x]$.

   (b) Find the additive inverse for $p(x)$ in $R[x]$.

   (c) Illustrate the commutative property of addition in $R[x]$ using the polynomials $p(x)$ and $q(x)$.

(d) Illustrate the associative property of addition in $R[x]$ using the polynomials $p(x), q(x)$, and $r(x)$.

(e) Verify that $p(x)q(x) = q(x)p(x)$.

(f) Assume that R has a multiplicative identity $u(x) = 1_R$. Verify that $p(x)u(x) = p(x)$.

Theorem 11.6 If R is a commutative ring, then $R[x]$ is a commutative ring. In addition, if the ring R has an identity, then the ring $R[x]$ has an identity. [see pp. 148-152 for the proof of this theorem]

Theorem 11.7 If R is a ring that contains zero divisors, then the polynomial ring $R[x]$ also contains zero divisors.

2. Let $R = \mathbb{Z}_6$. Let $f(x) = [2]x^2 + x + [5]$ and $g(x) = [3]x + 2$.

   (a) Compute and simplify the product $f(x)g(x)$.

   (b) What is the degree of the product $f(x)g(x)$? How does this compare to $\deg(f(x)) + \deg(g(x))$?

Theorem 11.10 Let m and n be non-negative integers. If D is an integral domain, then the product of polynomials of degree m and n in $D[x]$ is a polynomial in $D[x]$ of degree $(m + n)$.

Proof Sketch: Suppose $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x^1 + a_0x^0$ and $q(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_2x^2 + b_1x^1 + b_0x^0$ with $a_n \neq 0$ and $b_n \neq 0$. Then the product of the leading terms is $(a_n x^n)(b_m x^m) = (a_n b_m)(x^n x^m) = (a_n b_m)x^{n+m}$. Since D is an integral domain, $a_n b_m \neq 0$. Hence $\mathrm{deg(p(x)q(x) = n + m}$.

Corollary 11.11 If D is an integral domain then $D[x]$ is an integral domain.

3. Give the statement of a weaker result than Theorem 11.10 that is true when R is a commutative ring but not necessarily an integral domain. [Hint: What is the degree of $(f(x))^2$ if $f(x) = [2]x + [1]$ in $\mathbb{Z}_4$?]