Math 476 - Abstract Algebra 1
Day 34 Group Assignment

Name:____________________________________

Polynomial Rings and Divisibility

Definition 11.12 Let R be a commutative ring and let $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x + a_0$ be a polynomial in $R[x]$. The **polynomial function induced by *p(x)*** is the function $\overline{p} : R \to R$, where for each r in R, $\overline{p}(x) = a_n r^n + a_{n-1}r^{n-1} + \cdots a_1 r + a_0$. For simplicity, we often just say that $\overline{p}$ is a **polynomial function**.

1. Let $p(x) = x^4$ and $q(x) = x^2$ be polynomials in $\mathbb{Z}_5$.

   (a) For the polynomial function $\overline{p} : \mathbb{Z}_5 \to \mathbb{Z}_5$, determine $\overline{p}([0])$, $\overline{p}([1])$, $\overline{p}([2])$, $\overline{p}([3])$, and $\overline{p}([4])$.

   (b) For the polynomial function $\overline{q} : \mathbb{Z}_5 \to \mathbb{Z}_5$, determine $\overline{q}([0])$, $\overline{q}([1])$, $\overline{q}([2])$, $\overline{q}([3])$, and $\overline{q}([4])$.

   (c) Is the function $\overline{p}$ equal to the function $\overline{q}$? Explain.

2. Let $p(x) = x^4$ and $q(x) = x^2$ be polynomials in $\mathbb{Z}_4$.

   (a) For the polynomial function $\overline{p} : \mathbb{Z}_4 \to \mathbb{Z}_4$, determine $\overline{p}([0])$, $\overline{p}([1])$, $\overline{p}([2])$, and $\overline{p}([3])$.

   (b) For the polynomial function $\overline{q} : \mathbb{Z}_4 \to \mathbb{Z}_4$, determine $\overline{q}([0])$, $\overline{q}([1])$, $\overline{q}([2])$, and $\overline{q}([3])$.

   (c) Is the function $\overline{p}$ equal to the function $\overline{q}$? Explain.

3. We know that if R is a commutative ring, then $R[x]$ is a commutative ring, and that if R has identity, then $R[x]$ also has identity. We also know that if D is an integral domain, then $D[x]$ is also an integral domain. The next question to consider is: if F is a field, is $F[x]$ a field?

   (a) Is $\mathbb{R}[x]$ a field? (Hint: consider the polynomial $p(x) = x$ in $\mathbb{R}[x]$)

   (b) Is $\mathbb{Z}_3[x]$ a field?

   (c) If F is a field, if $F[x]$ always, sometimes, or never a field? Give a proof or appropriate examples.

Definition 12.2 Let R be a commutative ring and let $u(x)$ and $v(x)$ be polynomials in $R[x]$. The polynomial $u(x)$ **divides** the polynomial $v(x)$ provided that there exists a polynomial $q(x) \in R[x]$ such that $v(x) = u(x)q(x)$. In this case, we say that $u(x)$ is a **factor** of $v(x)$ and sometimes write $u(x)|v(x)$.

Theorem 12.3 Let F be a field and let $f(x), g(x) \in F[x]$.

- If $f(x)$ divides $g(x)$, and $c \in F$ and $c \neq 0$, then $cf(x)$ divides $g(x)$.
- If $f(x) \neq 0, g(x) \neq 0$, and $f(x)$ divides $g(x)$, then $\deg(f(x)) \leq \deg(g(x))$.
- If $f(x) \neq 0$ and a_n is the leading coefficient of $f(x)$, then $a_n^{-1}f(x)$ is a monic polynomial.
- If $f(x)$ divides $g(x)$ and $g(x)$ divides $f(x)$, then there exists $c \in F$ with $c \neq 0$ such that $f(x) = cg(x)$.
- Let $f(x)$ and $g(x)$ be monic polynomials in $F[x]$. If $f(x)$ divides $g(x)$ and $g(x)$ divides $f(x)$, then $f(x) = g(x)$.

Proof: The first and third parts of this theorem are proven on pp. 154-155 in your textbook. The proofs are fairly elementary – making use of the definition of divisibility on a polynomial ring and the existence of multiplicative inverses in a field. You should read and be familiar with these arguments. The proofs of the remaining parts are eligible presentation problems.

The Division Algorithm Let F be a field and let $f(x)$ and $g(x)$ be polynomials in $F[x]$ with $g(x) \neq 0$. There there exist unique polynomials $q(x)$ and $r(x)$ in $F[x]$ such that $f(x) = g(x)q(x) + r(x)$ and $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$.

4. Let $f(x) = x^4 + x^3 + 2x^2 + x + 2$ and $g(x) = 2x^2 + x + 1$ be polynomials in $\mathbb{R}[x]$. Use long division of polynomials to find polynomials $q(x)$ and $r(x)$ such that $f(x) = g(x)q(x) + r(x)$ with $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$. Does $g(x)$ divide $f(x)$?

5. Let $f(x) = x^4 + x^3 + [2]x^2 + x + [2]$ and $g(x) = [2]x^2 + x + [1]$ be polynomials in $\mathbb{Z}_3[x]$. Use long division of polynomials to find polynomials $q(x)$ and $r(x)$ such that $f(x) = g(x)q(x) + r(x)$ with $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$. Does $g(x)$ divide $f(x)$ in $\mathbb{Z}_3[x]$?

6. Let $f(x) = x^4 + x^3 + [2]x^2 + x + [2]$ and $g(x) = [2]x^2 + x + [1]$ be polynomials in $\mathbb{Z}_5[x]$. Use long division of polynomials to find polynomials $q(x)$ and $r(x)$ such that $f(x) = g(x)q(x) + r(x)$ with $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$. Does $g(x)$ divide $f(x)$ in $\mathbb{Z}_5[x]$?