Math 476 - Abstract Algebra 1
Day 36 Group Assignment **Name:**_____

Recall: An **ideal** I in a ring R is a subring of R such that $rx \in I$ and $xr \in I$ for all $r \in R$ and $x \in I$.

1. Let $R = \mathbb{Z}$ and consider the ideal $k\mathbb{Z} = \{kz : z \in \mathbb{Z}\}$ for some fixed positive integer k. Prove that $k\mathbb{Z}$ is an ideal (in which case we can conclude that it is a principle ideal).

2. Let $R = \mathbb{Z}$ and let I be an ideal of $\mathbb{Z}$.

   (a) If I is the trivial ideal, explain why I is a principal ideal.

   (b) Assume that I is a non-trivial ideal. Use the fact that I contains a non-zero element b to show that I contains a positive integer. (Hint: The integer b is either positive or negative).

   (c) Let $S = \{x \in I : x > 0\}$. Explain why S contains a smallest element a.

   (d) Prove that $\langle a \rangle \subseteq I$.

   (e) Let $y \in I$. Use the division algorithm to divide y by a. Use the fact that I is an ideal to show that the remainder r must be an element of I.

   (f) Since $r \in I$, what can we conclude about r, and why does this imply that $I \subseteq \langle a \rangle$?

Theorem 16.8 Every ideal of $\mathbb{Z}$ is a principal ideal. (Note: the content of the previous exercise proves this theorem).

Definition 16.9 An integral domain R is a **principal ideal domain** (PID) is every ideal R is a principal ideal.

Theorem 16.10 Let F be a field. Then $F[x]$ is a principal ideal domain.

Proof: The proof of this result can be found on p. 220 of your book. The outline of the proof is similar to the proof of theorem 16.8. After considering the case of the trivial ideal in $F[x]$, show that any non-trivial ideal contains a least monic polynomial. Show the principal ideal generated by this element is contained in the ideal. Then use the division algorithm and a similar argument that above to show that the remainder must be zero, giving the reverse containment. This shows equality, hence any ideal is principal.

Definition 16.17 Let R be a ring and I an ideal of R. The element $a \in R$ is **congruent modulo** I to $b \in R$ if $b - a \in I$.

3. Let $R = \mathbb{Z}_{12}$ and $I = \langle 3 \rangle$

   (a) Find all elements of R that are congruent to $[0]$ modulo I.

   (b) Find all elements of R that are congruent to $[1]$ modulo I.

   (c) Find all elements of R that are congruent to $[2]$ modulo I.

Claim: Congruence modulo I is an equivalence relation on R.

4. Let $R = \mathbb{Z}_{12}$ and $I = \langle 3 \rangle$

   (a) Find all of the elements of R/I.

   (b) Construct the addition table for R/I.

   (c) Construct the multiplication table for R/I.

   (d) What structure does R/I appear to have?

Definition 16.36 Let R and S be rings. A function $\varphi : R \to S$ is a **homomorphism** of rings if $\varphi(a+b) = \varphi(a)+\varphi(b)$ and $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$.

As we did in the context of group homomorphisms, certain types of homomorphisms are given special names:

- If φ is a homomorphism and an injection (1-1) then φ is called a **monomorphism**.
- If φ is a homomorphism and a surjection (onto) then φ is called an **epimorphism**.
- If φ is a homomorphism and a bijection then φ is called a **isomorphism**.

5. For each of the following, determine whether or not the given function is a homomorphism. If the function is a homomorphism, determine whether or not it is a monomorphism, epimorphism, or isomorphism.

   (a) Let $n \in \mathbb{Z}^+$, $n > 1$ and let $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ be defined by $\varphi(k) = [k]$.

   (b) Let R be a field and $r \in R$. Let $ev_r : R[x] \to R$ be defined by $ev_r(f(x)) = f(r)$.

   (c) Let $\varphi : \mathbb{Z}_{12} \to \mathbb{Z}_6$ be defined by $\varphi([k]_{12}) = [4k]_6$.