Dartmouth College
Mathematics 81

The following exercises are intended to remind you of (or sharpen your skills regarding) material from Math 71. When convenient we shall denote the quotient ring $\mathbb{Z}/m\mathbb{Z}$ by $\mathbb{Z}_m$. Also, recall that all our ring homomorphisms take the multiplicative identity of one ring to the multiplicative identity of the other.

1. Show that there exist ring homomorphisms $\mathbb{Z}_m \to \mathbb{Z}_n$ if and only if $n \mid m$. **Hint:** The first isomorphism theorem makes one implication almost effortless. Note that all such homomorphisms must be surjective.

2. The following exercise is meant to deepen your understanding of ideals and quotient rings. For each of the ideals I listed below, determined whether the ring $\mathbb{Z}[x]/I$ has zero divisors, is an integral domain, or is a field (and hence whether the ideal I is prime, maximal, or neither). If the quotient is not an integral domain, find zero divisors. If the quotient is not a field, then I is not maximal, so find a maximal ideal M with $I \subsetneq M$, and justify that M is maximal.

   First, here are a few results which you may use without proof, but if they are unfamiliar, you should read the relevant material in your text.

   Let $f \in \mathbb{Z}[x]$. f is called *primitive* if and only if the gcd of its coefficients is 1. For example $2x^2 - 6x + 3$ is primitive in $\mathbb{Z}[x]$. The following two theorems are essentially (if not in fact) equivalent to Gauss's lemma over $\mathbb{Q}$:

   Theorem: Let $f \in \mathbb{Z}[x]$. Then f is irreducible in $\mathbb{Z}[x]$ if and only if f is primitive in $\mathbb{Z}[x]$ and irreducible in $\mathbb{Q}[x]$.

   Theorem: Let $f \in \mathbb{Z}[x]$, and suppose that $f = gh$ for two polynomials $g, h \in \mathbb{Q}[x]$. Then $f = g_0 h_0$ for polynomials $g_0, h_0 \in \mathbb{Z}[x]$ with $\deg(g) = \deg(g_0)$ and $\deg(h) = \deg(h_0)$. In particular g_0 and h_0 are integer scalar multiples of g and h respectively.

   Hint: You may also use without proof the very handy fact that if $f \in \mathbb{Z}[x]$ and $m \in \mathbb{Z}$, then $\mathbb{Z}[x]/(m, f(x)) \cong (\mathbb{Z}/m\mathbb{Z})[x]/(\bar{f}(x))$, where $\bar{f}(x)$ is the polynomial in $(\mathbb{Z}/m\mathbb{Z})[x]$ obtained from f by reducing the coefficients modulo m.

   (a) $I = (x^3 + 2)$
   (b) $I = (5, x^3 + 2)$
   (c) $I = (7, x^3 + 2)$

3. Let $\mathbb{F}_{11} = \mathbb{Z}_{11} = \mathbb{Z}/11\mathbb{Z}$ be a (actually the) field with 11 elements, and set $K = \mathbb{F}_{11}[x]/(x^2 + 1)$ and $L = \mathbb{F}_{11}[y]/(y^2 + 2y + 2)$.

   (a) Show that K and L are both fields with 121 elements.
   (b) For $p(x) \in \mathbb{F}_{11}[x]$, let $\overline{p(x)}$ denote its image in K. Show that the map from $K \to L$ which takes $\overline{p(x)} \mapsto \overline{p(y+1)}$ is well-defined and a ring homomorphism. Finally show that the map is an isomorphism.