Solutions to Assignment 3

1. Check that the only idempotents in $\mathbb{Z}$ are 0 and 1.

Solution: If k is an integer and $k^2 = k$, then $k(k-1) = 0$. Now, if $a \cdot b = 0$ for integers a and b, then either $a = 0$ or $b = 0$. Thus, if $k \neq 0$ then this means $k - 1 = 0$ or $k = 1$.

2. For what integers n can you find idempotents *different from* 0 and 1 in $\mathbb{Z}/n$?

Solution: If a is an element of $\mathbb{Z}/n$ and $a^2 = a$ in this ring, then *treating a as an integer*, we have $n|(a^2 - a)$.

If n is prime, and $n|ab$, then either $n|a$ or $n|b$. So, in this case $n|a(a-1)$ means that either $n|a$ (i. e. $a = 0$ in $\mathbb{Z}/n$) or $n|(a-1)$ (i. e. $a = 1$ in $\mathbb{Z}/n$).

On the other hand, if $n = c \cdot d$ where c and d are positive and have no common factor, then by Chinese Remainder Theorem, one can find an integer a so that $c|a$ and $d|(a-1)$ (note that a and $a - 1$ have no common factor other than 1). In that case, $a^2 - a$ is divisible by n but neither a nor $a - 1$ is divisible by n.

Actually, in this case we can also give an alternate argument which avoids Chinese Rmainder Theorem. Since c and c have no common factor greater than 1, we can write $cA + dB = 1$ for suitable integers A and B. We now take $a = cA$ and note that $c|a$ and $d|(a-1)$.

In summary, the only integers n for which there is an idempotent different from 0 and 1 in $\mathbb{Z}/n$ are composite numbers n.

3. Given any ring R we have a natural ring homomorphism $f : \mathbb{Z} \to R$. For any element a in R and any integer n, check that $f(n) \cdot a = a \cdot f(n)$.

Solution: The natural homomorphism has the property that $f(1) = 1$ the multiplicative identity of R. This shows that $f(1) \cdot a = a = a \cdot f(1)$ Now,

$$0 = f(0) = f(1 + (-1)) = f(1) + f(-1)$$

So we see that $f(-1) = -1$, the additive inverse of 1 in R. We have already shown that $(-1) \cdot a = -a = a \cdot (-1)$ for all a in R. Thus, we get $f(-1) \cdot a = -a = a \cdot (-1)$. Similarly,

$$f(0) \cdot a = 0 \cdot a = 0 = a \cdot 0 = a \cdot f(0)$$

We now claim the following, which we have already proved for $n = 1$.

For every positive integer n, $f(n) \cdot a$ is the sum of n copies of a in R. Similarly, $a \cdot f(n)$ is the sum of n copies of a in R, $f(-n) \cdot a$ is the sum of n copies of $-a$ in R and so is $a \cdot f(-n)$.

This can be proved by induction on n. Suppose that we have already proved this for $n - 1 \geq 1$. We then write,

$$f(n) \cdot a = f((n-1)+1) \cdot a = (f(n-1)+f(1)) \cdot a = f(n-1) \cdot a + f(1) \cdot a = f(n-1) \cdot a + a$$

Now the first term on the right is the sum of $(n-1)$ copies of a, hence the right-hand side is the sum of n copies of a. (The crucial step is the use of the distributive law in the third equality.) The other cases are proved in a similar fashion.

The result follows from the claim.

4. Given an element a in a ring R consider the two "new" elements $b = 2 + 3 \cdot a$ and $c = a - 5 \cdot a^3$. Check that $b \cdot c$ has the form $n_0 + n_1 \cdot a + n_2 \cdot a^2 + n_3 \cdot a^3 + n_4 \cdot a^4$. How did you use the previous exercise in solving this one?

Solution: Using the distributive and associative laws we write

$$b \cdot c = (2 + 3 \cdot a) \cdot (a - 5 \cdot a^3) = 2 \cdot a - 10 \cdot a^3 + 3 \cdot a^2 + 3 \cdot a \cdot (-5) \cdot a^3$$

For the last term we will use the previous exercise and then we can simplify to

$$b \cdot c = 2 \cdot a + 3 \cdot a^2 - 10 \cdot a^3 - 15 \cdot a^4$$

5. Write down the formulas for addition and multiplication of $p(T) = p_0 + p_1 T + \cdots + p_k T^k$ and $q(T) = q_0 + q_1 T + \cdots + q_l T^l$. Here k and l are non-negative integers and p_i's and q_j's are elements of a ring R.

Solution: We use the distributive law to get

$$p(T) \cdot q(T) = \sum_{i=0}^{k} \sum_{j=0}^{l} p_i T^i q_j T^j$$

Now use the fact that $a \cdot T = T \cdot a$ for all a in R to get

$$p(T) \cdot q(T) = \sum_{i=0}^{k} \sum_{j=0}^{l} p_i q_j T^{i+j} \sum_{n=0}^{k+l} (\sum_{i=0}^{k} p_i q_{n-i}) \cdot T^n$$

The addition rule is much easier

$$p(T) + q(T) = \sum_{i=0}^{\max(k,l)} (p_i + q_i)T^i$$

where by convention we put p_i outside the range $i = 0, \ldots, k$ to be 0 and q_j outside the range $j = 0, \ldots, l$ to be 0.

6. (Starred) For a ring S and a fixed element s in S, define a map $D_s(a) = s \cdot a - a \cdot s$. This is *not* a ring homomorphism. However, check that $D_s(a+b) = D_s(a) + D_s(b)$ and (more importantly) $D_s(a \cdot b) = a \cdot D_s(b) + D_s(a) \cdot b$.

Solution: We check, using the distributive law and commutativity of addition, that

$$D_s(a+b) = s \cdot (a+b) - (a+b) \cdot s = s \cdot a - a \cdot s + s \cdot b - b \cdot s = D_s(a) + D_s(b)$$

Similarly, using the associativity of multiplication and commutativity of addition, we have

$$D_s(a \cdot b) = s \cdot (a \cdot b) - (a \cdot b) \cdot s = (s \cdot a) \cdot b - (a \cdot s) \cdot b + a \cdot (s \cdot b) - a \cdot (b \cdot s) = D_s(a) \cdot b + a \cdot D_s(b)$$

7. Suppose that R is commutative and that S is an R-algebra. Show that giving an element of S is the same as giving a homomorphism $R[T] \to S$ where the map is the natural one on R.

Solution: We are given that there is a homomorphism $R \to S$ so that the image of R (multiplicatively) commutes with all elements of S.

Given an element s in S, we can define a homomorphism $R[T] \to S$ by sending a polynomial $p(T) = a_0 + a_1 T + \cdots + a_k T^k$ to the element $a_0 + a_1 \cdot s + \cdots + a_k \cdot s^k$. Using the above formulas for addition and multiplication of polynomials one can check that this is a homomorphism. Note that T is mapped to s and that the identity $a \cdot T = T \cdot a$ is preserved under this mapping.

Conversely, given a homomorphism $R[T] \to S$ which is the given homomorphism on the elements of R (which are the "constant" polynomials in $R[T]$), we can associate to this homomorphism the element s which is the element to which T is mapped by the homomorphism. It then follows that T^k is mapped to s^k and thenc that the polynomial $p(T)$ as above is mapped exactly as given above.

8. Suppose $a \cdot b \neq b \cdot a$ in R, then show that the map $R[T] \to R$ which sends T to a is *not* a homomorphism.

> **Solution:** Let us denote this map by f.
>
> In order to be a homomorphism, it must preserve multiplication. Now, the image of T is a and the image of b is b. However, the product
>
> $$f(T) \cdot f(b) = a \cdot b \neq b \cdot a = f(b \cdot T) = f(T \cdot b)$$
>
> is not preserved.

9. Check that point-wise addition and multiplication make $\text{Map}(X, R)$ into a ring for any set X

> **Solution:** The required laws for addition and multiplication only need to be check point-wise. These point-wise cases are a consequence of the same laws for R.

10. For each element a in R we can consider the "constant" function $\underline{a}$ which sends every element of X to a. Show that this gives a ring homomorphism $R \to \text{Map}(X, R)$.

> **Solution:** We just check that the point-wise addition and multiplication of constant functions results in constant functions!

11. Check that evaluation gives a ring homomorphism $R[T] \to \text{Map}(R, R)$ when R is commutative.

> **Solution:** We note that T maps to the identity map $i : R \to R$. This gives an element of $\text{Map}(R, R)$ and thus, as seen above, this gives a homomorphism $R[T] \to \text{Map}(R, R)$. We only need to check that this homomorphism is the "evaluation map". By pointwise multiplication we see that T^k goes to the function that sends b to $i(b)^k = b^k$. Now a polynomial $p(T) = a_0 + \cdots + a_k T^k$ goes to the function that sends b to
>
> $$a_0 + a_1 \cdot i(b) + \cdots a_k i(b)^k = a_0 + a_1 \cdot b + \cdots a_k b^k$$
>
> In other words, this *is* the evaluation map.

12. (Starred) Does the above statement hold if R is not commutative? Give an example to justify your answer.

Solution: Suppose $a \cdot b \neq b \cdot a$ in R. If $i : R \to R$ denotes the identity map and $a : R \to R$ denotes the constant map with value a, then $a \cdot i - i \cdot a$ is a non-zero map it has a non-zero value on b. However, $a \cdot T = T \cdot a$ in $R[T]$. Hence, the evaluation map is not a homomorphism.

13. How many elements are there in the set $\mathrm{Map}(\mathbb{Z}/n, \mathbb{Z}/n)$?

Solution: Since we are only looking at *set-theoretic* maps, only the cardinality of the range and domain matters. Hence, the answer is n^n.

14. For $n = 3, 4, 5, 6$, find an explicit *non-zero* polynomial $p(T)$ in $(\mathbb{Z}/n)[T]$ for which $e_p(k) = 0$ for *every* element k in $\mathbb{Z}/n$.

Solution: Consider the polynomial

$$p(T) = T \cdot (T-1) \cdots (T-5)$$

It is clear that this polynomial vanishes on every element of $\mathbb{Z}/n$ for $n = 3, 4, 5, 6$. Moreover, the coefficient of T^6 in $p(T)$ is 1 and hence it is a non-zero polynomial.

15. Find an explicit *non-zero* polynomial $p(T)$ in $(\mathbb{Z}/n)[T]$ for which $e_p(k) = 0$ for *every* element k in $\mathbb{Z}/n$.

Solution: Consider the polynomial

$$p(T) = T \cdot (T-1) \cdots (T-(n-1))$$

It is clear that this polynomial vanishes on every element of $\mathbb{Z}/n$. Moreover, the coefficient of T^n in $p(T)$ is 1 and hence it is a non-zero polynomial.