Math 412 Homework 3

Submission Instructions: You are responsible to read these instructions. Failure to submit correctly as described below will result in point deductions or loss of credit for entire problems. Submit these problems on Gradescope by Thursday, February 8th, at 11:59pm. Each problem should be on a separate page (or pages). **You will need to scan a PDF of the assignment AND select the pages belonging to each problem when you submit on gradescope.**

1. Let $R = \text{Fun}(\mathbb{R}, \mathbb{R})$ be the ring in exercise D2 of the "Ring Basics" adventure sheet. 0_R and 1_R are the constant functions zero and one.

   Show which of the following subsets of R are subrings of R. If they are not subrings, show whether they are rings (with a different multiplicative identity than 1_R, but endowed with the same operations as in R) or not.

   (a) The set C of constant functions.

   (b) The set S of those functions f such that $f(q) = 0$ for any $q \in \mathbb{Q}$.

   (c) The set T consisting of 0_R, together with those functions with no zeros, or only a finite number of zeros. (A zero of a function $f \in R$ is an element $x \in \mathbb{R}$ such that $f(x) = 0$)

(a) C is a subring of R. Indeed, addition and multiplication of constant functions is a constant function, so C is closed under addition and multiplication. $0_R, 1_R \in C$. The additive inverse of the constant function of constant value $r \in$ is the constant function of constant value $-r \in$, so C is also closed under additive inverses.

(b) S is not a subring of R. The multiplicative identity is not contained in that subset.

S is a ring. Indeed, the definition of S implies that it is closed under addition and multiplication. Moreover,

- Addition and multiplication in S are associative because they are associative in R.
- Addition in S is commutative because it is commutative in R.
- 0_R is the additive identity in S because it is the additive identity in R and $0_R \in S$ (identities are unique).
- Let $f \in R$. $-f$, its additive inverse in R, is defined as $(-f)(x) = -f(x)$ for all $x \in$. Hence, $(-f)(q) = 0$ for all $q \in$, so $-f \in S$. Thus, every element in S has an additive inverse.
- The multiplicative identity is the function 1_S defined as

$$1_S(x) = \begin{cases} 0 & \text{if } x \in \\ 1 & \text{if } x \in \setminus \end{cases}$$

- Addition and multiplication are related by the distributive properties in S, as they are related by the distributive properties in R.

This concludes the proof that S is a ring under addition and multiplication, but not a subring of R.

(c) $\underline{T \text{ is not a subring or a ring}}$, as it is not closed under addition. For example, let f be the following element of T:

$$f(x) = \begin{cases} 0 & \text{if } x = 0 \\ -1 & \text{else} \end{cases}$$

Note that $1_R \in T$. However, $1_R + f \neq 0_R$ and has an infinite number of zeros, so $1_R + f \notin T$.

2. An element x in a ring R is said to be *nilpotent* if $x^m = 0_R$ for some positive integer m. Generalizing the definition on page 40 of our text, a *unit* u in a ring R is an element with a multiplicative inverse, meaning there exists $s \in R$ such that $su = us = 1_R$.

   (a) Prove that if $x \in R$ is nilpotent (and R is not the zero ring), then x cannot be a unit.

   (b) Prove that if $x \in R$ is nilpotent, then $(1_R - x)$ is a unit. (Hint: One approach to showing something is a unit is to write down its inverse. In this case, it could help to recall geometric series from Calculus.)

   (c) Describe all the nilpotent elements in $\mathbb{Z}_n$ in terms of their prime factorization.

(a) If x is a unit then we have $sx = xs = 1_R$ for some s. Then $0_R = x^n = x^n s^n = (xs)^n = 1_R$, which can't happen if R is not the zero ring.

(b) Suppose $x^n = 0$. Then $(1_R - x)(1_R + x + x^2 + \cdots + x^{n-1}) = 1_R - x^n = 1_R$

(c) $[a]_n$ is a nilpotent element if and only if the set of distinct prime factors of a is a superset of the distinct prime factors of n.

3. An element $r \neq 0$ in a commutative ring R is said to be a *zerodivisor* if there exists a nonzero element $s \in R$ such that $rs = 0$.

   (a) Given a nonzero element $r \in R$, prove that r is not a zerodivisor if and only if the map $R \longrightarrow R$ given by multiplication by r, meaning the map $s \mapsto rs$, is injective.

   (b) Describe all the zerodivisors in $\mathbb{Z}_n$ in terms of the prime factorization of n or their greatest common divisor with n.

(a) Suppose that r is not a zerodivisor, and consider $a, b \in R$ such that $ra = rb$. Then $r(a - b) = 0$, and since r is not a zerodivisor, we must have $a - b = 0$. This shows that multiplication by r is injective. On the other hand, if multiplication by r is an injective map, then $ra = 0$ implies that $a = 0$, and r is not a zerodivisor.

(b) If $m \in \mathbb{Z}$ is such that $[m]$ is a zerodivisor in $\mathbb{Z}_n$, that means $n \nmid m$ and there exists some $k \in \mathbb{Z}$ such that $n \nmid k$ but $n \mid km$. Equivalently, $1 < (n, m) < n$.

We will show in problem 4(e) that if $(n, m) = 1$, then m is a unit, and in problem 4(a) that units are not zerodivisors. If $1 < d = (n, m) < m$, then $n = dk$ for some $1 < k < n$, so $k \not\equiv 0 \mod n$, and $mk \equiv 0 \mod n$.

4. For two rings, R and S a function $\varphi\colon R \to S$ is a *ring homomorphism* if $\varphi(1_R) = 1_S$, and for all $x, y \in R$ the following conditions hold

$$\varphi(x +_R y) = \varphi(x) +_S \varphi(y), \text{ and } \varphi(x \times_R y) = \varphi(x) \times_S \varphi(y)$$

(a) Let R be any ring (recalling how our class convention differs from that of the book!). Prove that there exists a unique ring homomorphism $\mathbb{Z} \to R$.

(b) Let $n > 1$ be an integer. Prove that there does not exist a ring homorphism $\mathbb{Z}_n \to \mathbb{Z}$.

(c) Suppose R and S are two rings, and $f : R \to S$ is a ring isomorphism; in particular, f is a bijection and so has an inverse function $g : S \to R$. Prove that g is also a ring homomorphism.

(d) Prove the following theorem that appears in our worksheets:

If $f : R \to S$ is a ring homomorphism, then f is injective if and only if $\ker f = \{0_R\}$.

(a) We must prove that (1) **there exists** a ring homomorphism $f : \mathbb{Z} \to R$, and (2) this homomorphism is unique.

(1) Let $1_R \in R$ be the multiplicative identity. For $n \in \mathbb{Z}$, if $n \geq 0$ we define $f(n) = n1_R$, meaning we add 1_R to itself n times. If $n < 0$, we define $f(n) = -(-n)1_R$. Then $f(1) = 1_R$, $f(a+b) = (a+b)1_R = a1_R+b1_R = f(a)+f(b)$, and similarly $f(ab) = ab1_R = ab1_R1_R = (a1_R)(b1_R) = f(a)f(b)$, so f is indeed a ring homomorphism.

(2) Let $g : \mathbb{Z} \to R$ be any ring homomorphism. Then $g(1) = 1_R$, and $g(n) = g(1+\cdots+1) = n \cdot 1_R$ for all $n \geq 0$, so $g(n) = f(n)$ whenever $n \geq 0$. Now if $n < 0$, $0_R = g(0) = g(-n+n) = g(-n) + g(n) = (-n)1_R + g(n)$, where we are using that $-n > 0$ so $g(-n) = (-n)1_R$. But then $(-n)1_R = -g(n)$, since $g(n)$ has one additive inverse. Thus, $g(n) = f(n)$ for all $n \in \mathbb{Z}$.

(b) The proof is by contradiction. Suppose we have a ring homomorphism $f : \mathbb{Z}_n \to \mathbb{Z}$. Then $f([1]_n) = 1 \in \mathbb{Z}$, and $f([0]_n) = 0 \in \mathbb{Z}$. Because $[0]_n = [n]_n$, we know $f([n]_n) = f([0]_n) = 0$. But we also know $[n]_n = [1]_n + \cdots + [1]_n$ (i.e. $[1]_n$ added to itself n times), so $f([n]_n) = n \cdot 1 \neq 0$ since $\mathbb{Z}$ is an integral domain. But $0 \neq 1$ in $\mathbb{Z}$, a contradiction.

(c) We already know $f(1_R) = 1_S$, since f is a ring homomorphism, so $g(1_S) = 1_R$. We still need to show $g(st) = g(s)g(t)$, and $g(s+t) = g(s) + g(t)$, for all $s, t \in S$. Since f is a bijection, there are unique elements $a, b \in R$ with $f(a) = s$ and $f(b) = t$, which is to say $g(s) = a$ and $g(t) = b$. Then

$$\begin{aligned} g(st) &= g(f(a)f(b)) \\ &= g(f(ab)) \quad \text{since } f \text{ is a ring hom} \\ &= ab \quad \text{since } g \text{ is the inverse of } f \\ &= g(s)g(t). \end{aligned}$$

The proof that $g(s+t) = g(s) + g(t)$ is very similar.

(d) Suppose f is injective, so that $f(x) = f(y) \implies x = y$. Then suppose $f(x) = 0$. Then since $f(0) = 0$ we have $f(x) = f(0)$ and so $x = 0$. Now suppose $\ker f = 0$, and suppose $f(x) = f(y)$. Then $f(x) - f(y) = 0$ so $f(x-y) = 0$ so $x - y \in \ker f$ and $x - y = 0$. Then $x = y$.

(e) Suppose $f(x) = 0_R$ and $x \neq 0_k$. Then x has a multiplicative inverse x^{-1}, so we have $1_R = f(1_k) = f(xx^{-1}) = f(x)f(x^{-1}) = 0_R f(x^{-1}) = 0_R$, giving us a contradiction. Then $x = 0$ and by part (a), f is injective.