Homework Assignment 10 Solutions

1. Let R be a ring. Recall that for $a \in R$ we denote the *additive* inverse of a by $-a$. Establish the following identities.

   (a) $(-a)b = a(-b) = -ab$

   Proof. We'd like to prove that $(-a)b$ is the additive inverse of ab. It suffices (by HW2 problem 7) to show that $(-a)b + ab = 0$. Applying the distributive law:

   $$(-a)b + ab = (-a + a)b = 0b = 0.$$

   Similarly, we observe that:

   $$a(-b) + ab = a(-b + b) = a0 = a.$$

   These together give the result. □

   (b) $(-a)(-b) = ab$

   Proof. By part (a), we compute:

   $$(-a)(-b) = -((a)(-b)) = -(-ab) = ab.$$

   For the last step we use that in any group, the inverse of the inverse of an element is itself. □

   (c) If $1 \in R$ then $(-1)a = -a$.

   Proof. This follows immediately from part (a) and the fact that 1 is the multiplicative identity:

   $$(-1)a = -(1a) = -a.$$

   □

   (d) Suppose R is an integral domain. Show that if $a^2 = 1$ then $a = \pm 1$.

   Proof. Notice that factoring (or FOILing) is just applying the distributive law twice. Therefore, since $a^2 - 1 = 0$ so we can factor to get:

   $$(a - 1)(a + 1) = 0.$$

   Since R is an integral domain, it has no zero divisors, so that either $a-1 = 0$ or $a+1 = 0$. In the first case $a = 1$ and in the second $a = -1$. □

2. Let R be a ring with $1 \neq 0$.

   (a) Let $R^\times \subseteq R$ be the set of units of R. Show that $R^\times$ is a group under the multiplication operation of R.

Proof. We first show that multiplication is a well defined group operation on $R^\times$. This means that if $r, s \in R^\times$, we must show their product is too. Since r is a unit, there exists $r^{-1} \in R$ such that $rr^{-1} = r^{-1}r = 1$, and similarly for s. Then we see that $s^{-1}r^{-1}$ is an inverse for rs. Indeed:

$$(rs)(s^{-1}r^{-1}) = r1r^{-1} = 1 \quad \text{and} \quad (s^{-1}r^{-1})rs = s^{-1}1s = 1.$$

Therefore $rs \in R^\times$ and so multiplication is well defined. Multiplication in $R^\times$ is associative by the ring axioms. The multiplicative identity $1 \in R$ is a unit (indeed, its inverse is 1), so $R^\times$ has an identity. To see that inverses exists, observe that if $r \in R^\times$, then so is r^{-1} (its inverse is r). □

(b) Suppose that $a \in R$ is a zero divisor. Show that $a \notin R^\times$.

Proof. We prove the contrapositive. Let $a \in R^\times$, so that there there exists some (two-sided) multiplicative inverse a^{-1} to a. If $ab = 0$ then we can multiply on the left by a^{-1} and se that

$$b = a^{-1}ab = a^{-1}0 = 0.$$

Therefore $b = 0$. Similarly, if $ba = 0$ we can multiply on the right by a^{-1} to observe that $b = 0$. In either case, we have seen that we cannot multiply a by anything nonzero and get 0, so a is not a zero divisor. □

(c) Suppose R is a subring of some ring S. Show that if $a \in R^\times$ then $a \in S^\times$. Give an example to show the converse is false.

Proof. Let $a \in R^\times$. Then there exists some $a^{-1} \in R$ such that

$$aa^{-1} = a^{-1}a = 1 \tag{1}$$

Since $R \subseteq S$, we see that $a^{-1} \in S$ as well, and Equation (1) still holds, so that $a^{-1} \in R^*$. To see a counterexample, consider the subring $\mathbb{Z} \subseteq \mathbb{Q}$. Certainly $2 \in \mathbb{Z}$ is a unit in $\mathbb{Q}$, but not in $\mathbb{Z}$ (because its inverse, $\frac{1}{2}$ is rational but not an integer). ERRATA: This is not actually true in Dummit and Foote's definition of subring. Notice that I assumed here that the identity of R is the same as the identity of S (some authors require this in the definition of a subring). Consider, for example, $\mathbb{Z} \times \{0\} \subseteq \mathbb{Z} \times \mathbb{Z}$ (where addition multiplication in the latter is computed coordinatewise). Then the identity of the subring is $(1, 0)$, but the identity of the entire ring is $(1, 1)$. And so $(1, 0) \in (\mathbb{Z} \times \{0\})^\times$, but notice $(1, 0)(0, 1) = (0, 0)$ so that $(1, 0)$ is a zero divisor in $\mathbb{Z} \times \mathbb{Z}$, and therefore cannot be a unit. □

3. Let R be a commutative ring. An element $r \in R$ is called *nilpotent* if there exists a positive n such that $r^n = 0$. A commutative ring is called *reduced* if it has no nonzero nilpotent elements.

(a) Show that a nilpotent element of a ring is either 0 or a zero divisor.

Proof. If $a \neq 0$ is nilpotent, then $a^n = 0$ for some n. In fact, one can let n be the minimal number with this property, so that $a^{n-1} \neq 0$. Then $aa^{n-1} = 0$ but both $a, a^{n-1} = 0$, so a is a zero divisor. □

(b) Give an example of a ring with a nonzero nilpotent element.

Proof. Consider $3 \in \mathbb{Z}/9\mathbb{Z}$. It is nonzero but $3^2 = 9 \equiv 0 \mod 3$. More generally one can find nilpotents in $\mathbb{Z}/n\mathbb{Z}$ for any n that is not square free.
Another example is in the matrix ring $M_2(F)$ for a field F. Once can consider the nonzero matrix

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

and easily observe that its square is 0. □

(c) Show that the sum of nilpotent elements is nilpotent.

Proof. We first observe that if $a^n = 0$, then $a^r = 0$ for any $r \geq n$. Indeed,

$$a^r = a^n a^{r-n} = 0a^{r-n} = 0$$

Now suppose a and b are nilpotent. So $a^n = 0$ and $b^m = 0$. Fix any $r > 2\max(m, n)$. Then by the binomial formula:

$$(a+b)^r = \sum_{i=0}^{r} \binom{r}{i} a^i b^{r-i}.$$

Notice that one of i or $r - i$ is $\geq r/2 > \max(m, n) \geq m, n$, so that either $a^i = 0$ or else $b^{r-i} = 0$. Since this is true for each i, this shows $(a + b)^r = 0$ as desired. □

(d) Suppose r is nilpotent. Show that rx is nilpotent for all $x \in R$. (*Note*, in future terminology, (c) and (d) prove that the set of nilpotent elements is an *ideal* of R, which we will call the *nilradical*).

Proof. Suppose $r^n = 0$. Since R is commutative, then $(rx)^n = r^n x^n = 0x^n = 0$. □

(e) Suppose R is a commutative ring with $1 \neq 0$, and suppose $r \in R$ is nilpotent. Show that $1 + r \in R^\times$.

Proof. Suppose $r^n = 0$. Define an element $s \in R$ as the sum:

$$s = 1 - r + r^2 - r^3 + \cdots + (-1)^{n-1} r^{n-1}.$$

Then we compute (the telescoping sum):

$$(1+r)(1 - r + r^2 - r^3 + \cdots + (-1)^{n-1} r^{n-1}) \quad = \quad 1 + (-1)^{n-1} r^n = 1.$$

As R is commutative, this shows that $(1 + r)^{-1} = s$ so it is a unit. □

4. (a) Let $\{S_i \subseteq R\}$ be a nonempty collection of subrings of R. Show that $\bigcap_i S_i$ is a subring of R.

Proof. We already know it is an abelian subgroup (HW4 Problem 2(d)), so it suffices to show it is closed under multiplication. Given r and s in the intersection, we know r and s are in S_i for each i. Therefore so is rs since each S_i is a subring, and we win. □

(b) Suppose S is a subring of R, and R is a subring of T. Show that S is a subring of T.

Proof. We know S is an abelian subgroup of T, and it is closed under multiplication as a subgroup of R, so we are done. □

5. For a ring R, define the *center* of R to be:

$$Z(R) = \{r \in R \mid ra = ar \text{ for all } a \in R\}.$$

(a) Show that $Z(R)$ is a subring of R.

Proof. First we show that $Z(R)$ is an abelian subgroup of R. Let $r, s \in Z(R)$. We show $r - s \in Z(R)$ and apply the subgroup criterion (HW4 Problem 1(a)). For any $x \in R$, we use the distributive law and the fact that r, s are in the center, together with 1(a) above, to compute:

$$x(r-s) = xr + x(-s) = xr - xs = rx - sx = rx + (-s)x = (r-s)x.$$

Therefore $r - s \in Z(R)$. We next observe that $rs \in Z(R)$. Indeed:

$$xrs = rxs = rsx.$$

□

(b) Suppose R has $1 \neq 0$. Show that $R^\times \cap Z(R) \subseteq Z(R^\times)$. (The converse is *not true* in general, but I don't consider this to be obvious. Perhaps we will see an example later).

Proof. Suppose $r \in R^\times \cap Z(R)$. Then for any $x \in R^\times \subseteq R$ we know $xr = rx$. Therefore r is in the center of the subgroup $R^\times$. □

(c) Show that the center of a division ring is a field.

Proof. Fix $r \neq 0$. By assumption we know it has an inverse. We begin by observing that if $r \in Z(R)$, then so is r^{-1}. Indeed, Letting $r^{-1}x = y$ we multiply on the left by r to see that $x = ry = yr$ where the last equality is because r is in the center. Then we can multiply on the right by r^{-1} to conclude that $xr^{-1} = y$ also, so that r^{-1} and x commute. Since x was arbitrary, we've shown that $r^{-1} \in Z(R)$. In particular, any nonzero element of $Z(R)$ has an inverse, so $Z(R)$ is a field. □

(d) Let $\mathbb{H}$ be Hamilton's quaternions (defined in Lecture 21 or [DF] Example 5 on Page 224). Compute $Z(\mathbb{H})$. (Notice that $\mathbb{H}$ contains a copy of $\mathbb{C}$, is this the center?)

Proof. We begin by observing that any scalar is in the center by definition. Now fix an arbirary element $a + bi + cj + dk$ in the center. Since a itself is in the center, and the center is a subgroup, then after subtracting a we see that $bi + cj + dk$ is in the center. We then compute:

$$i(bi + cj + dk) = bi^2 + cij + dik = -b - dj + ck.$$

$$(bi + cj + dk)i = bi^2 + cji + dki = -b + dj - ck.$$

Since we are assuming these are in the center, these are equal, so their difference is 0. In particular, we see that:

$$(d+d)j - (c+c)k = 0.$$

So $d+d=0$ and $c+c=0$. Since they are real nubmers we see that $d=c=0$. We have therefore shown that our arbitrary element of the center is bi for some b. Now multiply on the left and right by j.

$$(bi)j = bk$$

$$j(bi) = -bk$$

As above, this show $b+b=0$ so that $b=0$. Since $b=c=d=0$ we see that the only elements of the center are scalars. In summary:

$$Z(\mathbb{H}) = \mathbb{R}.$$

□

6. Let R be ring, and X any set. Define

$$\text{Maps}(X,R) = \{f : X \to R \mid f \text{ is a function}\}.$$

Define binary operations $+$ and $\times$ as follows.

$$(f+g)(x) = f(x)+g(x) \qquad (f\times g)(x) = f(x)g(x).$$

(a) Show that $\text{Maps}(X,R)$ is a ring.

Proof. We first must show it is an abelian group. Let $\mathbf{0} : X \to R$ be the function that takes every element to 0, that is, $\mathbf{0}(x) = 0 \in R$ for all $x \in X$. Then for every $f \in \text{Maps}(X,R)$, and $x \in X$, we have

$$(\mathbf{0}+f)(x) = \mathbf{0}(x)+f(x) = f(x) = f(x)+\mathbf{0}(x) = (f+\mathbf{0}(x)). \tag{2}$$

Therefore $\mathbf{0}$ is an additive identity. We next show associativity. Associativity in $\text{Maps}(X,R)$ follows from that in R. Indeed: for any $f,g,h \in \text{Maps}(X,R)$ and $x \in X$ we compute:

$$((f+g)+h)(x) = (f(x)+g(x))+h(x) = f(x)+(g(x)+h(x)) = (f+(g+h))(x). \tag{3}$$

Since this holds for each x, we obtain associativity. To see that inverses exist, given f we define $-f$ by the rule $(-f)(x) = -f(x)$ (where the latter is the additive inverse of $f(x)$ in R). Then it is clear that

$$(f+(-f))(x) = f(x)-f(x) = 0 = \mathbf{0}(x).$$

We similarly observe that $-f+f=\mathbf{0}$. Finally, the additive structure is abelian because the addive structure on R is. Indeed, given $f,g \in \text{Maps}(X,R)$, we know that for each $x \in X$:

$$f(x)+g(x) = g(x)+f(x) \tag{4}$$

We now must consider the multiplicative structure. We first observe associativity, arguing exactly as in Equation (3), but with $+$ replaced by $\times$. Finally, the distributive law follows from that in R. Indeed, for each $f,g,h \in \text{Maps}(X,R)$, and $x \in X$:

$$(f(g+h))(x) = f(x)(g(x)+h(x)) = f(x)g(x)+f(x)h(x) = (fg+fh)(x).$$

Distributivity on the other side follows identically. I will point out that I probably went into more detail than is strictly necessary. One needs only observe that each of the ring axioms can be checked after evaluating at an arbitrary point x, and that the hold there because they hold in R. Nevertheless, as parts (e) and (f) below indicate, one must be careful in considering which properties can be checked after evaluating at a point. □

(b) Suppose R is commutative, show that $\mathrm{Maps}(X, R)$ is too.

Proof. Whether 2 functions f and g commute can be checked after evaluating at an arbitrary point x, whence the result follows arguing as in Equation (4), but with $+$ replace by $\times$. □

(c) Suppose R is unital, show that $\mathrm{Maps}(X, R)$ is too.

Proof. Define the function $\mathbf{1} : X \to R$ by the rle $\mathbf{1}(x) = 1$ for all $x \in X$ (where 1 is the additive identity of R). Then one checks that $\mathbf{1}f = f\mathbf{1} = f$ for all $f \in \mathrm{Maps}(X, R)$ after evaluating at an arbitrary $x \in X$, whence the result follows arguing as in Equation 2 replacing $\mathbf{0}$ with $\mathbf{1}$ and $+$ with $\times$. □

(d) Suppose R is reduced (defined in Problem 3), show that $\mathrm{Maps}(X, R)$ is too.

Proof. Suppose f is a nilpotent element of $\mathrm{Maps}(X, R)$, so that $f^n = \mathbf{0}$ for some positive integer n. Then for any x, we have $f(x)^n = 0$. Since R is reduced, its only nilpotent element is 0, so that $f(x) = 0$. Since x was arbitrary, this shows that $f = \mathbf{0}$ to begin with. Therefore the only nilpotent element of $\mathrm{Maps}(X, R)$ is the zero map, proving that it is reduced. □

(e) Give an example to show that even if R is a field, $\mathrm{Maps}(X, R)$ need not be.

Proof. The important observation is that if $f : X \to R$ is any function, and $f(x) = 0$ for any x, then f cannot be a unit in $\mathrm{Maps}(X, R)$. Indeed, if f had an inverse g, then $fg = \mathbf{1}$ implies that $f(x)g(x) = 1$, but since $f(x) = 0$, this isn't possible. Therefore any nonzero function which is has a zero is an example of a nonunit. In particular, if X is any set with more than one element, then $\mathrm{Maps}(X, R)$ is not a field, as we can construct f by the rule $f(x) = 0$ for a fixed $x \in X$, and $f(y) = 1$ for all $y \neq x$, and it won't be a unit. □

(f) Give an example to show that even if R is an integral domain, $\mathrm{Maps}(X, R)$ need not be.

Proof. The idea of the proof is the same as part (e). Namely, that a function can be "locally zero" (ie, evaluate to 0 at some points) but not "globally zero" (ie, the 0 function). Indeed, fix $f, g : X \to R$. If $fg = \mathbf{0}$, then this says that $f(x)g(x) = 0$ for all $x \in X$. Since R is an integral domain, then either $f(x) = 0$ or $g(x) = 0$. The important observation is that f can be 0 at some points, and g can be 0 at other points, so that neither has to be the 0 function.

The simplest concrete example is the following. Let $X = \{x, y\}$ be a 2 point set, and R any integral domain. Then define f, g by the rules:

$$f(x) = 0 \qquad g(x) = 1$$
$$f(y) = 1 \qquad g(y) = 0.$$

Then it is clear that neither f or g are 0, but their product is at both x and y, so that $fg = \mathbf{0}$. □

7. We now develop an example of rings that appear along the intersection of the algebraic and analytic theory (for example in *functional analysis*). You may use without proof the following facts from elementary calculus: **(1)** If f, g are continuous so are their sum and product. **(2)** If f, g are differentiable then they are continuous and:

$$(f+g)' = f' + g' \qquad (fg)' = f'g + fg'$$

(a) Let $\mathscr{P}$ be a property of maps from $X \to R$, and let

$$\text{Maps}_{\mathscr{P}}(X, R) = \{f : X \to R \mid f \text{ has property } \mathscr{P}\}.$$

Suppose that the 0 map has property $\mathscr{P}$. Suppose also that if f and g have property $\mathscr{P}$, then so do $f - g$ and $f \times g$. Show that $\text{Maps}_{\mathscr{P}}(X, R)$ is a subring of $\text{Maps}(X, R)$.

Proof. Since the 0 map has $\mathscr{P}$, then $\text{Maps}_{\mathscr{P}}(X, R)$ is nonempty. Since it is closed under subtraction, it is an abelian subgroup (by HW4 Problem 1a). Then it is a subring because it is closed under multiplication. □

(b) Let $X = R = \mathbb{R}$. Let $f : \mathbb{R} \to \mathbb{R}$ have property $\mathscr{C}^0$ if f is continuous, and define $C^0(\mathbb{R}) = \text{Maps}_{\mathscr{C}^0}(\mathbb{R}, \mathbb{R})$ to be the set of continuous functions from $\mathbb{R}$ to $\mathbb{R}$. Use part (a) to show that $C^0(\mathbb{R})$ is a subring of $\text{Maps}(\mathbb{R}, \mathbb{R})$.

Proof. We know from intro calculus that the 0 function is continuous. We also know that if f is continuous, so is $-f$. Therefore if f, g are continuous, so are $f - g$ and fg. Therefore the set of continuous maps form a subring by part (a). □

(c) For each $n > 0$ let $f : \mathbb{R} \to \mathbb{R}$ have property $\mathscr{C}^n$ if f has a derivative everywhere, and df/dx has propery $\mathscr{C}^{n-1}$. (So for example, f is $\mathscr{C}^1$ if it is differentiable and its derivative is continuous). Show by induction on n that $C^n(\mathbb{R}) = \text{Maps}_{\mathscr{C}^n}(\mathbb{R}, \mathbb{R})$ is a subring of $C^{n-1}(\mathbb{R})$.

Proof. It is useful to have an alternative characterization of $\mathscr{C}^n$.

Lemma 1. *A function f is $\mathscr{C}^n$ if and only if $d^i f/dx^i$ exists and is continuous for $i = 0, 1, \cdots, n$.*

Proof. We prove this by induction. The base case $\mathscr{C}^0$ is trivial. For the general case, then f is $\mathscr{C}^n$ if and only if df/dx exists and is $\mathscr{C}^{n-1}$. By induction, this holds if and only if the j'th derivatives of df/dx exist and are continuous of $i = 0, \cdots, n-1$, which is equivalent to the $j+1$st derivatives of f existing and being continuous for $j = 0, \cdots, n-1$. Letting $i = j + 1$ then gives the result □

A trivial consequence of Lemma 1 is that $C^n(\mathbb{R}) \subseteq C^{n-1}(\mathbb{R})$ We must show it is closed under subtraction and multiplication. We proceded by induction, noting that the base case for $n = 0$ is part (b). For the general case, fix $f, g \in C^n(\mathbb{R})$. Then $f - g$ is differentiable, and its derivative is $f' - g'$. Since both $f', g' \in C^{n-1}(\mathbb{R})$, their difference is as well (by induction), so this shows that $f - g \in C^n(\mathbb{R})$. Now consider fg. We know it is differentiable, and its derivative is $f'g + fg'$. As before f' and g' are $\mathscr{C}^{n-1}$, and since $C^n(\mathbb{R}) \subseteq C^{n-1}(\mathbb{R})$, so are f and g. Since $C^{n-1}(\mathbb{R})$ is a ring (by induction), we see that $f'g + fg' \in C^{n-1}(\mathbb{R})$, so that fg is $\mathscr{C}^n$, as desired. □

(d) A funcion $f : \mathbb{R} \to \mathbb{R}$ is has property $\mathscr{C}^\infty$ if for each positive n the n'th derivative of f exists and is continuous. (Such a function is also often called *smooth*). Show that $C^\infty(\mathbb{R}) = \text{Maps}_{\mathscr{C}^\infty}(\mathbb{R}, \mathbb{R})$ is a subring of $C^n(\mathbb{R})$ for each n. (Hint: rather than prove this directly, you could use (4)).

Proof. By Lemma 1, we see that $C^\infty(\mathbb{R}) = \bigcap_{d>0} C^d(\mathbb{R}) = \bigcap_{d>n} C^d(\mathbb{R})$. Therefore, since it is an intersection of subrings of $C^n(\mathbb{R})$, it is a subring of $C^n(\mathbb{R})$ by 4(a). □

8. Let A be an abelian group (written additively). Define the *endomorphism ring* of A as follows:

$$\text{End}(A) = \{f : A \to A \mid f \text{ is a homomorpism}\}.$$

Give $\text{End}(A)$ 2 binary operations $+$ and $\times$ as follows:

$$(f + g)(a) = f(a) + g(a) \qquad (f \times g)(a) = f(g(a)).$$

(a) Prove that $\text{End}(A)$ is a ring.

Proof. We first show that $\text{End}(A)$ is an abelian group under $+$. This follows essentially identically to the computation in 6(a). The additive identity is the 0 map ($\mathbf{0}(a) = 0$), and the inverse is computed pointwise ($(-f)(a) = -f(a)$), and associativity and abelianness is inherited from A. We omit the details. The fact that multiplication is associative follows because composition of functions is associative. What remains is the distributive law. Fix homomorphisms $f, g, h : A \to A$. For all $a \in A$ we consider:

$$\begin{aligned}((f + g)h)(a) &= (f + g) \circ h(a) \\ &= f(h(a)) + g(h(a)) \\ &= ((fh) + (gh))(a)\end{aligned}$$

This was the easy side of the distributive law, and would work for any functions. On the other hand, the other direction of distributivity actually uses the fact that these are homomorphisms (in the third step below):

$$\begin{aligned}(f(g + h))(a) &= f \circ (g + h)(a) \\ &= f(g(a) + h(a)) \\ &= f(g(a)) + f(h(a)) \\ &= ((fg) + (fh))(a)\end{aligned}$$

As an interesting exercise, notice that if you just the set S_A of *permutations* of A which need not be homomorphisms, and try to make it into a ring with multiplication given by composition (as above), you get an object which satisfies the distributive law on the right, but not on the left! □

(b) Prove that $(\mathrm{End}(A))^\times \cong \mathrm{Aut}(A)$.

Proof. Notice that there is an obvious inclusion of sets $\mathrm{Aut}(A) \subseteq \mathrm{End}(A)$ (since every automorphism is automatically an endomorphism). Furthermore, an endomorphism $f : A \to A$ is a unit in the endomorphism ring if and only if it has an inverse as a function, that is, if and only if it is an automorphism of A. Therefore the inclusion exhibits a bijection

$$\mathrm{Aut}(A) \leftrightarrow \mathrm{End}(A)^\times.$$

Finally, since on both sides the group law is composition, it is in fact an isomorphism of groups. □

(c) Let E be an elementary abelian p-group of order p^n. Show that $\mathrm{End}(E) \cong M_n(\mathbb{F}_p)$ (You may use that $n \times n$ matrices over a field F correspond to linear maps $F^n \to F^n$. Compare to HW7 Problem 5).

Proof. This was a bonus, but the general idea is the following. We first notice that an elementary abelian p-group of order p^n is isomorphic to $\mathbb{F}_p^n$ (this is Definition/Proposition 4 on Takehome 2). By HW7 Problem 5 we know that an endomorphism of $\mathbb{F}_p^n$ is the same data as a linear map from $\mathbb{F}_p^n$ to itself. By linear algebra, this corresponds to a unique matrix in $M_n(\mathbb{F}_p)$. Furthermore, addition of endomorphisms corresponds to addition of matrices, and composition of endomorphisms corresponds to multiplication of matrices, so this identification indeed preserves the ring structure. □