Math 566 - Homework 2
SOLUTIONS
Prof Arturo Magidin

1. Let $(R,+,\cdot)$ be a ring, and let $(R^{\text{op}},+,\circ)$ be the opposite ring, as in Homework 1, Problem 1. Let I be a subset of R. Show that I is a left (resp. right) ideal of $(R,+,\cdot)$ if and only if I is a right (resp. left) ideal of $(R^{\text{op}},+,\circ)$

   Proof. Note that I is a subgroup of $(R,+)$ if and only if it is a subgroup of $(R^{\text{op}},+)$. So we may restrict our attention to subsets that are subgroups of R.

   Assume that I is a left ideal of R. It is a subgroup of R^{op} because the additive structure has not changed. Now if $x\in I$ and $r\in R$, then $x\circ r = rx\in I$, because I is a left ideal of R. Therefore, I is a right ideal of R^{op}. Conversely, if I is a right ideal of R^{op}, $x\in I$, and $r\in R$, then $rx = x\circ r\in I$ because I is a right ideal of R^{op}, so I is a left ideal of R.

   Since $(R^{\text{op}})^{\text{op}} = R$, the statement about right ideals of R now follows. □

2. Let R be a ring, and let X be a set. Let R^X be the set of all functions $f\colon X\to R$. Define addition and multiplication in R^X by

$$(f+g)(x) = f(x)+g(x), \qquad (fg)(x) = f(x)g(x)$$

   where the operations on the right hand side are the operations of R.

   (i) Prove that R^X with these operations is a ring.
   Proof. The ring R has underlying set that can be thought of as the product $\prod_{x\in X} R$, which is the set of all functions from X to R. This is an abelian group under coordinate-wise addition, which corresponds to pointwise addition; and is a semigroup under coordinatewise multiplication, which corresponds to pointwise multiplication. So the only thing that we need to check is that the product distributes over the sum.
   Indeed, given $f,g,h\in R^X$, and $x\in X$, we have

$$\begin{aligned}\big(f(g+h)\big)(x) &= f(x)(g+h)(x) = f(x)(g(x)+h(x)) = f(x)g(x)+f(x)h(x)\\ &= (fg)(x)+(fh)(x) = \big(fg+fh\big)(x),\\ \big((g+h)f\big)(x) &= (g+h)(x)f(x) = (g(x)+h(x))f(x) = g(x)f(x)+h(x)f(x)\\ &= (gf)(x)+(hf)(x) = \big(gf+hf\big)(x).\end{aligned}$$

   Thus, we have a ring. □

$$(a_x)\Big((b_x)+(c_x)\Big) = (a_x)(b_x+c_x) = \big(a_x(b_x+c_x)\big) = \big(a_xb_x+a_xc_x\big) = (a_x)(b_x)+(a_x)(c_x),$$

   and similarly for $(a_x+b_x)(c_x) = (a_x)(c_x)+(b_x)(c_x)$. □

   (ii) Prove that R^X is commutative if and only if R is commutative or X is empty.
   Proof. If X is empty, then $R^X = \{\varnothing\}$ is the one element ring, which is commutative. If $X\neq\varnothing$ and R is commutative, then given $f,g\in R^X$ we have that for all $x\in X$,

$$(fg)(x) = f(x)g(x) = g(x)f(x) = (gf)(x),$$

   and therefore that $fg=gf$. Thus, R^X is commutative.
   Conversely, if X is nonempty and R^X is commutative, let $a,b\in R$. The constant functions $\mathbf{a},\mathbf{b}\colon X\to R$ given by $\mathbf{a}(x)=a$ and $\mathbf{b}(x)=b$ lie in R^X. Let $x\in X$; then

$$ab = \mathbf{a}(x)\mathbf{b}(x) = (\mathbf{ab})(x) = (\mathbf{ba})(x) = \mathbf{b}(x)\mathbf{a}(x) = ba,$$

   so $ab=ba$ and hence R is commutative. □

(iii) Prove that R^X has a unity if and only if R has a unity or X is empty.

Proof. If X is empty then R^X is the one element ring, which has unity equal to the additive identity. So assume $X \neq \varnothing$.

If R has a unity, let $\mathbf{1} \in R^X$ be the constant function $\mathbf{1}(x) = 1_R$. Then for all $f \in R^X$ and all $x \in X$, we have

$$f(x) = f(x)1_R = f(x)\mathbf{1}(x) = (f\mathbf{1})(x),$$

so $f = f\mathbf{1}$; symmetrically,

$$f(x) = 1_R f(x) = \mathbf{1}(x)f(x) = (\mathbf{1}f)(x),$$

so $f = f\mathbf{1} = \mathbf{1}f$, proving that $\mathbf{1}$ is the unity of R^X.

Conversely, let $\mathbf{1}$ be the unity of R^X, and let $x \in X$. I claim that $\mathbf{1}(x) \in R$ is the unity of R. Indeed, let $a \in R$ and let $\mathbf{a}$ be the constant function with value a. Then

$$a = \mathbf{a}(x) = \mathbf{a1}(x) = \mathbf{a}(x)\mathbf{1}(x) = a\mathbf{1}(x),$$

and

$$a = \mathbf{a}(x) = \mathbf{1a}(x) = \mathbf{1}(x)\mathbf{a}(x) = \mathbf{1}(x)a,$$

so $\mathbf{1}(x)$ is the unity of R^X, as claimed. $\square$

3. Let R and S be rings with unity, and let $f\colon R \to S$ be a ring homomorphism; recall that we do not require ring homomorphisms to be unital unless we specify that they are.

(i) Show that if $1_S \in \operatorname{Im}(f)$, then $f(1_R) = 1_S$.

Proof. Let $r \in R$ be such that $f(r) = 1_S$. Then

$$1_S = f(r) = f(r1_R) = f(r)f(1_R) = 1_S f(1_R) = f(1_R). \ \square$$

(ii) Prove that if there exists $u \in R$ such that $f(u)$ is a unit in S, then $f(1_R) = 1_S$.

Proof. Let $v \in S$ be such that $vf(u) = f(u)v = 1_S$. If $s \in S$, then

$$f(u)1_S = f(u) = f(u1_R) = f(u)f(1_R).$$

Now multiplying on the left by v we have $vf(u)1_S = vf(u)f(1_R)$. Since $vf(u) = 1_S$, we deduce $1_S = f(1_R)$, as claimed. $\square$

4. Let p be a prime number.

(i) Prove that if $1 \leq k \leq p-1$, then $\binom{p}{k}$ is a multiple of p.

Proof. Note that $\binom{p}{k} = \frac{p!}{k!(p-k)!}$. Since $k \leq p-1$, all factors of $k!$ are strictly smaller than p; and since $k \geq 1$, all factors of $(p-k)!$ are strictly smaller than p. Thus, the factor of p in the numerator does not cancel, so $\binom{p}{k} = \frac{p!}{k!(p-k)!} = p\left(\frac{(p-1)!}{k!(p-k)!}\right)$, with both factors integers. Thus, $\binom{p}{k}$ is divisible by p. $\square$

(ii) THE FRESHMAN'S DREAM. Let R be a commutative ring with identity such that we have $\operatorname{char}(R) = p$. Prove that for all $a, b \in R$ and positive integers n, $(a+b)^{p^n} = a^{p^n} + b^{p^n}$.

Proof. Induction on n. If $n = 1$, we have

$$(a+b)^p = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k} + b^p.$$

Since $\mathrm{char}(R) = p$, $px = 0$ for all $x \in R$. Therefore $\binom{p}{k} a^k b^{p-k} = 0$ if $1 \leq k \leq p-1$, and we get $(a+b)^p = a^p + b^p$, as claimed.

Assuming the result holds for n, we have

$$(a+b)^{p^{n+1}} = \left((a+b)^{p^n}\right)^p = (a^{p^n} + b^{p^n})^p = (a^{p^n})^p + (b^{p^n})^p = a^{p^{n+1}} + b^{p^{n+1}},$$

as claimed. $\square$

5. Let R be a ring. An element $r \in R$ is *nilpotent* if and only if there exists a positive integer n such that $r^n = 0$.

   (i) Show that if R is commutative, then the set of all nilpotent elements of R is an ideal of R.

   Proof. Let N be the set of all nilpotent elements. It is nonempty, since $0 \in N$. If $a, b \in N$, let $n > 0$ be such that $a^n = 0$, and let $m > 0$ be such that $b^m = 0$. Then

   $$(a-b)^{n+m} = a^{n+m} + \sum_{k=1}^{n+m-1} \binom{n+m}{k} (-1)^k a^{n+m-k} b^k + (-1)^{n+m} b^{n+m}.$$

   The first and last term are equal to 0, because the exponents of a and b are larger than n and m, respectively. If $1 \leq k \leq m$, then $a^{n+m-k} = 0$; if $m < k \leq n+m$, then $b^k = 0$. Thus, each term in the sum is equal to 0 as well. So $(a-b)^{n+m} = 0$, proving that N is a subgroup of R.

   Finally, if $a \in N$ and $r \in R$, let $n > 0$ be such that $a^n = 0$. Then

   $$(ra)^n = r^n a^n = r^n 0 = 0.$$

   Thus, N is an ideal, as claimed. (We only need to check one side because R is commutative.) $\square$

   (ii) Give an example of a ring R and elements a and b of R such that each of a and b are nilpotent, but neither ab nor $a+b$ are nilpotent. Hint: Try 2×2 matrices.

   Proof. Of course there are many possible examples. Here is one. Let $R = M_2(\mathbb{R})$ be the ring of 2×2 matrices with coefficients in $\mathbb{R}$, and let

   $$a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \qquad \text{and} \qquad b = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

   Then $a^2 = b^2 = 0$. However, we have that

   $$a+b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \text{and} \qquad ab = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

   Note that $a+b$ is invertible, hence cannot be nilpotent (in fact, $(a+b)^2 = I_2$). As for ab, $ab \neq 0$, but $(ab)^2 = ab$, so ab cannot be nilpotent either. Thus, the set of nilpotent matrices in R is not an ideal, subring, or even a subgroup. $\square$

6. Given a function $f\colon \mathbb{R} \to \mathbb{R}$, the *support of* f is the set

   $$\mathrm{supp}(f) = \{r \in R \mid f(r) \neq 0\}.$$

   We say f *has compact support* if and only if there exists $N > 0$ such that $\mathrm{supp}(f) \subseteq [-N, N]$.

   Let R be the ring of all functions $f\colon \mathbb{R} \to \mathbb{R}$ with pointwise addition and multiplication.

(i) Let S be the set of all elements of R that are continuous and have compact support. Prove that S is a subring of R.

Proof. Note that S is nonempty, since the function $f(x) = 0$ for all x lies in S.

We know that the sum, difference, and product of continuous functions is continuous. We just need to verify that the property of having compact support is also respected. Let f and g be continuous with compact support. Let $N, M > 0$ be such that $\mathrm{supp}(f) \subseteq [-N, N]$ and $\mathrm{supp}(g) \subseteq [-M, M]$. Let $K = \max\{N, M\}$. For $x \in \mathbb{R}$, if $|x| > K$ then $f(x) = g(x) = 0$. Thus, $\mathrm{supp}(f - g), \mathrm{supp}(fg) \subseteq [-K, K]$, proving that both the difference and product of elements of S is in S. Thus, S is a subring of R. $\square$

(ii) Prove that S does not have an identity, but nonetheless $S^2 = S$.

Proof. Careful; it is not enough to show that the unity of R does not lie in S, since we know that a subring could have a unity different from the unity of R.

So, first, let us prove that S does not have a unity. To that end, we show that if $f \in S$ and $f \neq 0$, then there exists $g \in S$ such that $g \neq 0$ but $fg = 0$. This will show that f cannot be a unity of S.

Let $f \in S$, $f \neq 0$. There exists N such that $\mathrm{supp}(f) \subseteq [-N, N]$.

Now let g be the function given by

$$g(x) = \begin{cases} 0 & \text{if } x \leq N+1 \\ x - (N+1) & \text{if } N+1 \leq x \leq N+2 \\ N+3-x & \text{if } N+2 \leq x \leq N+3 \\ 0 & \text{if } x \geq N+3. \end{cases}$$

Then $g \neq 0$, but $fg = 0$ since $\mathrm{supp}(f) \cap \mathrm{supp}(g) = \varnothing$.

On the other hand, let $h \in S$ be given by

$$h(x) = \begin{cases} 0 & \text{if } x \leq -(N+1) \\ x + N + 1 & \text{if } -(N+1) \leq x \leq -N \\ 1 & \text{if } -N \leq x \leq N \\ N+1-x & \text{if } N \leq x \leq N+1 \\ 0 & \text{if } N+1 \leq x. \end{cases}$$

Then $h(x) = 1$ for all $x \in [-N, N]$, so $hf = f$. In particular, since $hf \in S^2$, it follows that $f \in S^2$.

Since f was nonzero and arbitrary, we have that $S \subseteq S^2$, and hence that $S^2 = S$ even though S does not have a unity. $\square$

(iii) Prove that S is not an ideal of R.

Proof. The problem here is not the compact support, but the continuity. For example, let

$$f(x) = \begin{cases} 1 - |x| & \text{if } -1 \leq x \leq 1, \\ 0 & \text{otherwise.} \end{cases}$$

This function lies in S. Now let $g(x) = 1$ if $x \geq 0$ and $g(x) = -1$ if $x < 0$; this function lies in R. Then

$$(fg)(x) = \begin{cases} 0 & \text{if } x < -1, \\ -1 - x & \text{if } -1 \leq x < 0 \\ 1 - x & \text{if } 0 \leq x \leq 1 \\ 0 & \text{if } 1 < x. \end{cases}$$

In particular, $(fg)(0) = 1$, but as we approach 0 from the left the limit equals -1; that is, fg is not continuous at 0, and so is not an element of S. $\square$