Homework 1 Solutions

Enrique Treviño

February 11, 2019

Most problems below are from Judson.

1. Find all of the ideals in each of the following rings. Which of these ideals are maximal and which are prime?

   (a) $\mathbb{Z}_{18}$

   (b) $\mathbb{Z}_{25}$

   (c) $\mathbb{Q}$

   Solution 1.

   (a) The maximal ideals are $\{0, 2, 4, \ldots, 16\}$, $\{0, 3, 6, \ldots, 15\}$, and $\mathbb{Z}_{18}$. They are both also prime ideals. The rest of the ideals are $\{0\}, \{0, 6, 12\}, \{0, 9\}$.

   (b) The maximal (and prime) ideals are $\mathbb{Z}_{25}$ and $\{0, 5, 10, 15, 20\}$. The other ideal is $\{0\}$.

   (c) We'll prove the only ideals are $\{0, \}$, $\mathbb{Q}$. $\mathbb{Q}$ is maximal and prime, while $\{0\}$ is neither. Suppose there was an ideal $I \neq \{0\}$. Then I has an element $q \neq 0$. Since $q \in \mathbb{Q}$, then $\frac{1}{q} \in \mathbb{Q}$, but since I is an ideal and $q \in I$, then any multiplication of q times a rational is in I. Therefore $q\left(\frac{1}{q}\right) \in I$. So $1 \in I$, so $I = \mathbb{Q}$. Therefore there are only two ideals, $\{0\}$ and $\mathbb{Q}$.

2. Find all ring homomorphisms $\phi : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/15\mathbb{Z}$.

   Solution 2. Let $\phi : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/15\mathbb{Z}$ be a ring homomorphism. Then $\phi(0) = 0$. Let $\phi(1) = k$. Then

   $$0 = \phi(0) = \phi(1 + 5) = \phi(1) + \phi(5) = k + 5k = 6k.$$

   Therefore $6k \equiv 0 \bmod 15$. This means $k \equiv 0 \bmod 5$, therefore $k = 0, 5, 10$.

   Now using multiplicativity

   $$k = \phi(1) = \phi(1 \cdot 1) = \phi(1)\phi(1) = k^2.$$

   Therefore $k^2 \equiv k \bmod 15$. When $k = 0, 10$ we have $k^2 \equiv k \bmod 15$. When $k = 5$ we haave $k^2 \not\equiv k \bmod 15$. Therefore $k = 0$ or $k = 10$.

   The two possible ring homomorphisms are

   - $\phi(a) = 0$ for all a, and
   - $\phi(n) = 0, 10, 5, 0, 10, 5$ for $n = 0, 1, 2, 3, 4, 5$, respectively.

3. Let m, n be positive integers. How many ring homomorphisms are there from $\mathbb{Z}_m$ to $\mathbb{Z}_n$? Hint: Consider $d = \gcd(m, n)$.

   Solution 3. As done in the previous exercise, let $\phi(1) = k$. Then $\phi(a) = ak$. To satisfy additivity we need

   $$0 = \phi(0) = \phi(1 + (m - 1)) = \phi(1) + \phi(m - 1) = k + (m - 1)k = mk.$$

Therefore $mk \equiv 0 \bmod n$. Let $d = \gcd(m, n)$. Then

$$\left(\frac{m}{d}\right) k \equiv 0 \bmod \left(\frac{n}{d}\right),$$

but m/d and n/d don't share any factors (other than 1) so $k \equiv 0 \bmod n/d$. So we can write $k = r\frac{n}{d}$ for some $r \in \{0, 1, \ldots, d-1\}$.

To satisfy multiplicativity we need

$$r\frac{n}{d} = k = \phi(1) = \phi(1)\phi(1) = k^2 = r^2\left(\frac{n}{d}\right)^2.$$

Therefore

$$r\frac{n}{d} \equiv r^2\left(\frac{n}{d}\right)^2 \bmod n.$$

After dividing by n/d we get

$$r \equiv r^2\left(\frac{n}{d}\right) \bmod d.$$

Then

$$r\left(\frac{n}{d}r - 1\right) \equiv 0 \bmod d.$$

Now, r and $\frac{n}{d}r - 1$ are relatively prime, so they share no factors in common. If we do the prime factorization of d as

$$d = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_t^{\alpha_t}q_1^{\beta_1}q_2^{\beta_2}\cdots q_s^{\beta_s},$$

where the primes $q_1, q_2, \ldots, q_s$ are all the primes that divide d and n/d. Then there are 2^t possible ring homomorphisms. Namely solve the system of equations

$$\begin{aligned} r &\equiv 0 \bmod q_1^{\beta_1}\cdots q_s^{\beta_s}p_{i_1}^{\alpha_{i_1}}p_{i_2}^{\alpha_{i_2}}\cdots p_{i_h}^{\alpha_{i_h}} \\ \frac{n}{d}r &\equiv 1 \bmod p_{j_1}^{\alpha_{j_1}}p_{j_2}^{\alpha_{j_2}}\cdots p_{j_{t-h}}^{\alpha_{t-h}}, \end{aligned}$$

for each possible partition of the p_i's in two sets. There are 2^t ways of doing that, and there's a unique solution r modulo d for each choice, which in turn creates a unique k modulo n.

Finally we need to prove that each one of these is in fact a ring homomorphism. Suppose a k is picked using the above conditions, i.e., $mk \equiv 0 \bmod n$ and $k^2 \equiv k \bmod n$. Let's show this creates a ring homomorphism.

Let $a, b \in \mathbb{Z}_{\geqslant}$. Then $a + b = (a + b) \bmod m + m\ell$ for some integer ℓ and $ab = (ab) \bmod m + mg$ for some integer g. We have $\phi(a + b) = (a + b \bmod m)k \bmod n$ and $\phi(ab) = ((ab) \bmod mk^2 \bmod n$. Now

$$\begin{aligned} \phi(a) + \phi(b) &= ak + bk \bmod n = (a + b)k \bmod n \\ &= ((a + b) \bmod m)k + mk\ell \bmod n \equiv ((a + b) \bmod m)k \bmod n = \phi(a + b). \\ \phi(a)\phi(b) &= (ab)k^2 \bmod n = (ab \bmod m)k^2 + mgk^2 \bmod n \equiv \phi(ab) + mkg \bmod n = \phi(ab). \end{aligned}$$

4. Prove or disprove: The ring $\mathbb{Q}(\sqrt{2}\,) = \{a+b\sqrt{2} : a, b \in \mathbb{Q}\}$ is isomorphic to the ring $\mathbb{Q}(\sqrt{3}\,) = \{a+b\sqrt{3} : a, b \in \mathbb{Q}\}$.

Solution 4. Suppose $\phi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$ is a ring isomorphism. Since $\phi(0) = \phi(0+0) = \phi(0)+\phi(0)$, then $\phi(0) = 0$. Let $x = \phi(1)$. We have $x = \phi(1) = \phi(1 \cdot 1) = \phi(1)\phi(1) = x^2$. But $x \in \mathbb{Q}(\sqrt{3}) \subset \mathbb{R}$. Therefore we can solve $x^2 = x$ in the reals. The solutions are $x = 0$ and $x = 1$. If $x = 0$, then $\phi(a) = 0$ for all a, which is not a bijection. Therefore $\phi(1) = 1$. Then $\phi(2) = \phi(1 + 1) = \phi(1) + \phi(1) = 2$. Let $y = \phi(\sqrt{2})$. Then

$$2 = \phi(2) = \phi(\sqrt{2} \cdot \sqrt{2}) = \phi(\sqrt{2})\phi(\sqrt{2}) = y^2.$$

Therefore $y^2 = 2$. This means $y = \sqrt{2}$ or $y = -\sqrt{2}$. However, $\pm\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$, which is a contradiction. This means $\mathbb{Q}(\sqrt{2})$ is not isomorphic to $\mathbb{Q}(\sqrt{3})$.

For those wondering how do we know $\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$. Suppose $\sqrt{2} \in \mathbb{Q}(\sqrt{3})$, then there exist integers a, b, c, d with $b \neq 0, d \neq 0$ such that

$$\sqrt{2} = \frac{a}{b} + \frac{c}{d}\sqrt{3}.$$

Since $\sqrt{2}$ is irrational, then $c \neq 0$. Therefore

$$\begin{aligned} bd\sqrt{2} &= ad + bc\sqrt{3} \\ b(d\sqrt{2} - c\sqrt{3}) &= ad \\ b^2(2d^2 + 3c^2 - 2cd\sqrt{6}) &= a^2d^2 \\ \sqrt{6} &= \frac{a^2d^2 - 2b^2d^2 - 3b^2c^2}{-2b^2cd} \in \mathbb{Q}. \end{aligned}$$

But $\sqrt{6}$ is irrational, so we have a contrradiction.

5. Prove that the Gaussian integers, $\mathbb{Z}[i]$, are an integral domain.

Solution 5. Let's assume we already know that the Gaussian integers are a ring and let's prove that they are an integral domain. Suppose $x, y \in \mathbb{Z}[i]$ such that $xy = 0$. Let $x = a + bi$ and $y = x + di$. Then

$$0 = xy = (a + bi)(c + di) = (ac - bd) + (ad + bc)i.$$

Therefore

$$ac - bd = 0,$$

and

$$ad + bc = 0.$$

If $c = 0$, then $bd = 0$ and $ad = 0$. If $d = 0$, then $c + di = 0 + 0i = 0$, so $y = 0$ (and hence one of x and y is 0). If $d \neq 0$, then since $bd = 0$, $b = 0$; and because $ad = 0$, $a = 0$. Therefore $a + bi = 0 + 0i = 0$, so $x = 0$. Therefore if $c = 0$, one of x and y is zero.

Now let's take care of the case $c \neq 0$. Then $a = \dfrac{bd}{c}$ and so $\dfrac{bd^2}{c} = -bc$, implying $bd^2 = -bc^2$. If $b \neq 0$, then $d^2 = -c^2$. But $d^2 \geq 0$ and $c^2 \geq 0$. The only way $d^2 = -c^2$ is if $d = c = 0$, in which case $y = 0$. Since $c \neq 0$, then $b = 0$. But then

$$a = \frac{bd}{c} = \frac{0}{c} = 0,$$

so $x = a + bi = 0 + 0i = 0$.

In all cases, we have that either $x = 0$ or $y = 0$ and hence $\mathbb{Z}[i]$ is an integral domain.

Alternative Solution. Suppose $(a + bi)(c + di) = 0$ with $a + bi \neq 0$. Since $a + bi \in \mathbb{C}$ and $a + bi \neq 0$, then it has an inverse in $\mathbb{C}$ (namely $\frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$). By multiplying by the inverse we get $c + di = 0$. Therefore $\mathbb{Z}[i]$ is an integral domain.

Remark 1. The alternative solutions suggests that if R is a subring of a field $\mathbb{F}$, then R is an integral domain.

6. Let $\phi : R \to S$ be a ring homomorphism. Prove each of the following statements.

   (a) If R is a commutative ring, then $\phi(R)$ is a commutative ring.

   (b) $\phi(0) = 0$.

   (c) Let 1_R and 1_S be the identities for R and S, respectively. If ϕ is onto, then $\phi(1_R) = 1_S$.

   (d) If R is a field and $\phi(R) \neq 0$, then $\phi(R)$ is a field.

Solution 6.

(a) Let $\phi(r), \phi(s) \in \phi(R)$. We have $\phi(r)\phi(s) = \phi(rs) = \phi(sr) = \phi(s)\phi(r)$. Therefore $\phi(R)$ is commutative.

(b) $\phi(0) = \phi(0+0) = \phi(0) + \phi(0)$. Since S is a ring, then $\phi(0)$ has an additive inverse, therefore $\phi(0) = 0$.

(c) Let $s = \phi(1_R)$. Let r be such that $\phi(r) = 1_S$ (such an r exists because ϕ is onto). Then

$$1_S = \phi(r) = \phi(r \cdot 1_R) = \phi(r)\phi(1_R) = \phi(r)s = 1_S s = s.$$

Therefore $s = 1_S$, which is what we want to prove.

(d) Since R is a field, R is commutative, so $\phi(R)$ is commutative (by (a)). Suppose $\phi(1) = 0$, then $\phi(r) = \phi(r)\phi(1) = 0$ for all $r \in R$. This would contradict that ϕ is not the 0 function. Therefore $\phi(1) \neq 0$. Now let $\phi(r) \in \phi(R)$ such that $\phi(r) \neq 0$. Since $\phi(r) \neq 0$, $r \neq 0$. But then r has an inverse r^{-1}, so

$$\phi(1) = \phi(rr^{-1}) = \phi(r)\phi(r^{-1}).$$

Therefore $\phi(r)$ has an inverse in $\phi(R)$. Therefore $\phi(R)$ is a field.

7. Prove the Third Isomorphism Theorem for rings: Let R be a ring and I and J be ideals of R, where $J \subset I$. Then
$$R/I \cong \frac{R/J}{I/J}.$$

Solution 7. Let $\phi : R/J \to R/I$ be defined by $phi(r+J) = \phi(r+I)$. Let's show the map is well-defined. Suppose $r + J = s + J$. Then $r - s \in J \subseteq I$. Therefore $\phi(r+J) = r + I = s + I = \phi(s+J)$. The function is also a ring homomorphism because

$$\phi(r_1 + J) + \phi(r_2 + J) = (r_1 + I) + (r_2 + I) = (r_1 + r_2) + I = \phi(r_1 + r_2)$$
$$\phi(r_1 + J) \cdot \phi(r_2 + J) = (r_1 + I) \cdot (r_2 + I) = (r_1 \cdot r_2) + I = \phi(r_1 \cdot r_2).$$

Let $K = \ker(\phi)$, then $(R/J)/K \cong \phi(R/J)$. Suppose $r + I \in R/I$, then $\phi(r+J) = r + I$, therefore ϕ is onto, so $\phi(R/J) = R/I$.

Suppose $\phi(r+J) = 0 + I$, then $r \in I$. Therefore the elements in the kernel have the form $r + J$ where $r \in I$, i.e., the kernel is I/J.

The First Isomorphism Theorem now implies that $\frac{R/J}{I/J} \cong R/I$.

8. Let R be an integral domain. Show that if the only ideals in R are $\{0\}$ and R itself, R must be a field.

Solution 8. Let $a \neq 0$ be an element of R. Let $I = \langle a \rangle$. Since $a \neq 0$, then $I \neq \{0\}$. By assumption $I = R$. But that means $1 \in I$, so $1 \in \langle a \rangle$. That means there is an element $r \in R$ such that $1 = ar$, but that means a has an inverse. Therefore R is a field.

9. Let R be a commutative ring. An element a in R is **nilpotent** if $a^n = 0$ for some positive integer n. Show that the set of all nilpotent elements forms an ideal in R.

Solution 9. Let $\mathfrak{N}$ be the set of nilpotent elements of R. Let $a \in \mathfrak{N}$, and $b \in R$. There exists a non-negative integer n such that $a^n = 0$. Since R is commutative, then $(ab)^n = a^n b^n = 0$. Therefore $ab \in \mathfrak{N}$. This shows that it has the ideal property and that multiplication is closed. Also $(-a)^n = (-1)^n a^n = 0$, therefore $-a \in \mathfrak{N}$, which implies that every element has an additive inverse. $0^1 = 0$, so $0 \in \mathfrak{N}$. Finally, we need to show that for any $a, c \in \mathfrak{N}$, that $(a+c)^k = 0$ for some non-negative integer k. Since $a, c \in \mathfrak{N}$, then there exist nonnegative integer n, m such that $a^n = 0$ and $c^m = 0$.

Then
$$(a+c)^{m+n-1} = \sum_{j=0}^{m+n-1} \binom{m+n-1}{j} a^j c^{m+n-1-j}.$$

Note that when $j \geq n$, $a^j = 0$. When $j \leq n-1$, then $m + n - 1 - j \geq m$, so $c^{m+n-1-j} = 0$. Therefore $(a+c)^{m+n-1} = 0$.

Since $\mathfrak{N}$ is a subring and it satisfies the ideal property, then it is an ideal.

10. Let p be prime. Prove that

$$\mathbb{Z}_{(p)} = \{a/b : \ a, b \in \mathbb{Z} \text{ and } \gcd(b, p) = 1\}$$

is a ring. The ring $\mathbb{Z}_{(p)}$ is called the **ring of integers localized at** p.

Solution 10. Let $a/b, c/d, e/f \in \mathbb{Z}_{(p)}$. We want to show the following:

(a) $a/b + c/d \in \mathbb{Z}(p)$

(b) $(a/b)(c/d) \in \mathbb{Z}(p)$

(c) $(a/b) + (c/d + e/f) = (a/b + c/d) + e/f$

(d) $(a/b)(c/d + e/f) = (a/b)(c/d) + (a/b)(e/f)$

(e) $0 \in \mathbb{Z}(p)$

(f) $-(a/b) \in \mathbb{Z}(p)$

(g) $(a/b) + (c/d) = (c/d) + (a/b)$

The operations are the ones from $\mathbb{R}$, so they are commutative, associative and distributive. These gives us (c),(d),(g). $0 = 0/1$ and $\gcd(1, p) = 1$, so $0 \in \mathbb{Z}_{(p)}$. $-(a/b) = -a/b \in \mathbb{Z}_{(p)}$. We need only do (a) and (b).

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd},$$
$$\left(\frac{a}{b}\right)\left(\frac{c}{d}\right) = \frac{ac}{bd}.$$

Since $\gcd(b, p) = 1$ and $\gcd(d, p) = 1$, then $\gcd(bd, p) = 1$. Therefore $a/b + c/d$ and $(a/b)(c/d) \in \mathbb{Z}_{(p)}$