Mathematics 228(Q1), Assignment 9
Solutions

Exercise 1.(15 marks) (a) Let R be a ring with identity, and I an ideal of R.

(i) If $1 \in I$, prove $I = R$.

(ii) If I contains a unit, prove $I = R$.

(b) Let F be a field. If I is an ideal of F, show $I = (0)$ or $I = F$.

(c) Let R be a commutative ring with identity $1 \neq 0$. Suppose the only ideals of R are (0) and R. Show R is a field.(Hint : If $a \in R$ is non-zero, what can be said about the ideal (a) ? How does this help you find a multiplicative inverse of a ?)

Solution.(a)(i) Since I is an ideal containing 1, if $r \in R$ then

$$r = r \cdot 1 \in I.$$

It follows that $R \subseteq I$; the reverse inclusion is trivial, hence $I = R$.

(ii) Let u be a unit of R belonging to I. Since I is an ideal,

$$1 = u^{-1} \cdot u \in I.$$

Part (i) above allows us to conclude $I = R$.

(b) Suppose $I \neq (0)$. In this case, I contains a non-zero element u. Observing u is a unit, F being a field, part (a)(ii) allows us to conclude $I = F$.

(c) Let a be a non-zero element of the ring R and consider the principal ideal (a). Since $a = 1 \cdot a \in (a)$, the ideal (a) is non-zero, hence the given hypothesis ensures it equals R. In particular, (a) contains the identity element 1, i.e. there exists $b \in R$ such that

$$ba = 1.$$

Since R is commutative, we deduce a is a unit. Observing that a was an arbitrary non-zero element of R, we conclude R is a field.

Exercise 2.(10 marks)(a) If I and J are ideals in a ring R, show that their sum

$$I + J = \{a + b \,:\, a \in I, b \in J\}$$

is an ideal of R.

(b) Let d be the greatest common divisor of intergers a and b. Show that $a\mathbf{Z} + b\mathbf{Z} = d\mathbf{Z}$. (Hint : First show d belongs to the left-hand side.)

Solution.(a) Since I and J are ideals, they are non-empty. If $a \in I$ and $b \in J$ then

$$a + b \in I + J,$$

so $I + J$ is non-empty.

Let x, $y \in I + J$. By definition of the sum, there exists a, $c \in I$ and b, $d \in J$ such that

$$x = a + b \qquad \text{and} \qquad y = c + d.$$

Since I and J are ideals, we have $a + c$ and $-a$ both belong to I and $b + d$ and $-b$ both belong to J. Therefore,

$$x + y = (a + b) + (c + d) = (a + c) + (b + d)$$

and

$$-x = -(a + b) = (-a) + (-b)$$

both belong to $I + J$. This shows that $I + J$ is closed under addition and additive inverses. Finally, if $r \in R$ then $ra \in I$ and $rb \in J$, I and J being ideals, hence

$$rx = r(a + b) = ra + rb \in I + J.$$

(b) Recall that the greatest common divisor d of a and b can be written in the form

$$d = xa + yb$$

for suitable integers x and y. Observing $xa \in \mathbf{Z}a$ and $yb \in \mathbf{Z}b$, the definition of ideal sum allows us to conclude that

$$d = xa + yb \in \mathbf{Z}a + \mathbf{Z}b.$$

As $\mathbf{Z}a + \mathbf{Z}b$ is an ideal of $\mathbf{Z}$, we deduce that it contains every integral multiple of d, hence

$$\mathbf{Z}d \subseteq \mathbf{Z}a + \mathbf{Z}b.$$

On the other hand, suppose $z \in \mathbf{Z}a + \mathbf{Z}b$, say

$$z = ra + sb, \qquad r, s \in \mathbf{Z}.$$

Writing $a = nd$ and $b = md$, we deduce

$$z = r(nd) + s(md) = (rn + sm)d \in \mathbf{Z}d.$$

It follows that $\mathbf{Z}a + \mathbf{Z}b \subseteq \mathbf{Z}d$, hence

$$\mathbf{Z}d = \mathbf{Z}a + \mathbf{Z}b,$$

as required.

Exercise 3.(10 marks) Let J be an ideal in R. Show that

$$I = \{r \in R \,:\, rt = 0 \text{ for every } t \in J\}$$

is an ideal of R.

Solution. Since

$$0 \cdot t = 0$$

for all $t \in J$, we deduce $0 \in I$. In particular, I is non-empty.

Suppose a, b belong to I. If $t \in J$ then

$$(a + b)t = at + bt = 0 + 0 = 0.$$

This shows that I is closed under addition. Furthermore, observing that $t \in J$ implies $-t \in J$, J being an ideal, we also have

$$(-a)t = a(-t) = 0,$$

thus I is also closed under additive inverses. Finally, if $r \in R$ then, given $t \in J$,

$$(ra)t = r(at) = r \cdot 0 = 0.$$

We conclude ra also belongs to I.

Exercise 4.(10 marks) Let a, b be elements of an integral domain R. Show that $(a) = (b)$ if and only if a and b are associates. (Hint : Since R has an identity, $b \in (b) = (a)$ – what does this tell us about b ?)

Solution. Recall that an integral domain contains a unit 1. Therefore,

$$b = 1 \cdot b \in (b) = (a).$$

The definition of the principal ideal (a) allows to conclude there exists $u \in R$ such that

$$b = ua. \tag{$*$}$$

Reversing the roles of a and b, we deduce there exists $w \in R$ such that

$$a = wb.$$

Substituting for a in $(*)$, we deduce

$$1 \cdot b = b = (uw)b.$$

The fact R is an integral domain allows us to conclude $1 = uw$. In particular, u is a unit of R, hence $(*)$ shows that b is an associate of a.

On the other hand, suppose b is an associate of a, say $b = ua$ for some unit u of R. If $r \in R$ then

$$rb = r(ua) = (ru)a,$$

hence $(b) \subseteq (a)$. Since u is a unit,

$$a = u^{-1}b,$$

so the same argument yields $(a) \subseteq (b)$, hence $(a) = (b)$.

Exericse 5.(15 marks) Let p be a prime integer.

(a) Let T be the set of rational numbers that can be written in the form a/b, a, $b \in \mathbf{Z}$, with b not divisible by p. Show T is a subring of $\mathbf{Q}$.
(b) Let I be the subset of T consisting of elements a/b in which a is divisible by p. Show that I is an ideal of T.
(c) Show T/I is isomorphic to $\mathbf{Z}_p$. (Hint : By definition, if $t \in T$ then there exists integers a, b with p not dividing b such that $t = a/b$. Since b is relatively prime to p, $[b]$ is a unit of $\mathbf{Z}_p$. Consider the map

$$\phi : T \to \mathbf{Z}_p$$

defined by $\phi(a/b) = [a][b]^{-1}$.)

Solution.(a) T is non-empty, since it contains $0 = 0/1$. Suppose x, y are elements of T. By definition, there exists integers a, b, c, and d, with b and d not divisible by p, such that

$$x = \frac{a}{b} \qquad \text{and} \qquad y = \frac{c}{d}.$$

Using the rules for adding fractions, we calculate

$$x + y = \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

and

$$xy = \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Since it does not divide either b or d, the prime p does not divide the product bd. It follows that both $x + y$ and xy belongs to T. Furthermore,

$$-x = -\frac{a}{b} = \frac{-a}{b}$$

shows that $-x$ also belongs to T.

In summary, T is a non-empty subset of $\mathbf{Q}$ that is closed under addition, additive inverses, and multipication, i.e. it is a subring of $\mathbf{Q}$.

(b) Since 0 is divisible by p, $0 = 0/1$ belongs to I; in particular, I is non-empty. If x and y are elements of I then there exists integers a, b, c, and d, with a and c (respectively, b and d) divisible (respectively, not divisible) by p, such that

$$x = \frac{a}{b} \qquad \text{and} \qquad y = \frac{c}{d}.$$

Since

$$x + y = \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

has the property p divides $ad + bc$, we deduce $x + y$ belongs to I. Furthermore, the fact $p|a$ ensures $p| - a$, hence

$$-x = \frac{-a}{b}$$

also belongs to I. Thus, I is closed under addition and additive inverses.

Let $t \in T$, say $t = e/f$ where e, $f \in \mathbf{Z}$, $p \not| f$. If $x \in I$ is as above,

$$tx = \frac{e}{f} \cdot \frac{a}{b} = \frac{ea}{fb}.$$

Since it does not divide f and b, the prime p does not divide fb. Furthermore, since p divides a, it also divides the product ea. We deduce $tx \in I$, hence I is an ideal of T.

(c) We first observe that the map ϕ is well-defined. For suppose $x = a/b = a'/b'$ with a, a', b, b' are integers, b and b' relatively prime to p. Clearing denominators, we deduce

$$ab' = ab,$$

hence

$$[a][b'] = [ab'] = [a'b] = [a'][b].$$

Multiplication by $[b]^{-1}[b']^{-1}$ thus yields

$$[a][b]^{-1} = [a'][b']^{-1},$$

as required.

Using the notation introduced in part (a), let

$$x = \frac{a}{b} \qquad \text{and} \qquad y = \frac{c}{d}$$

be two elements of T. As the map $n \mapsto [n]$ is a homomorphism of $\mathbf{Z}$ onto $\mathbf{Z}_n$, we have

$$\begin{aligned}
\phi(x + y) &= \phi\left(\frac{ad + bc}{bd}\right) \\
&= [ad + bc][bd]^{-1} \\
&= ([a][d] + [b][c])\,([b][d])^{-1} \\
&= ([a][d] + [b][c])\,[b]^{-1}[d]^{-1} \\
&= [a][b]^{-1} + [c][d]^{-1} = \phi(x) + \phi(y),
\end{aligned}$$

and

$$\begin{aligned}
\phi(xy) &= \phi\left(\frac{ac}{bd}\right) \\
&= [ac][bd]^{-1} \\
&= [a][c]([b][d])^{-1} \\
&= [a][c][b]^{-1}[d]^{-1} \\
&= ([a][b]^{-1})([c][d]^{-1}) = \phi(x)\phi(y).
\end{aligned}$$

The preceding calculations shows that ϕ is a homomorphism.

If $x \in \ker \phi$ then

$$[0] = \phi(x) = \phi\left(\frac{a}{b}\right) = [a][b]^{-1}.$$

Multiplication by $[b]$ yields $[a] = [0]$, hence p divides a. Thus, $\ker \phi \subseteq I$. On the other hand, if $x \in I$ then the fact p divides a ensures

$$\phi(x) = [a][b]^{-1} = [0][b]^{-1} = [0],$$

hence $I \subseteq \ker f$. We conclude $I = \ker f$. Finally, ϕ is surjective. Indeed, recalling that $\mathbf{Z}_p$ consists of the elements $[n]$, $n \in \mathbf{Z}$, this is a consequence of the fact

$$[n] = \phi\left(\frac{n}{1}\right)$$

with $n/1 \in T$.

In light of the preceding discussion, the First Isomorphism Theorem allows us to conclude that ϕ induces an isomorphism of T/I with $\mathbf{Z}_p$.

Exercise 6.(10 marks) Let F be a field, R a non-zero ring, and $f : F \to R$ a surjective homomorphism. Prove that f is an isomorphism.(Hint : Exercise 1(b) may be helpful.)

Solution. Let K be the kernel of f. Since F is a field, exercise 1(b) asserts that K is either (0) or F. In the latter case, the definition of kernel would yield

$$\{0\} = f(F) = R,$$

the last equality following from the assumption f is surjective. Since this contradicts the assumption R is a non-zero ring, we conclude that $K = (0)$.

In particular, f is therefore injective. Since it was assumed to be a surjective homomorphism, we deduce f is an isomorphism.