Solution for Math 301 Homework 5

3.1

12. Let $\mathbb{Z}[i]$ denote the set $\{a + bi | a,\ b \in \mathbb{Z}\}$. Show that $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$.

Solution:

(1) For all $a + bi,\ c + di \in \mathbb{Z}[i]$, we have $(a + bi) + (c + di) = (a + c) + (b + d)i \in \mathbb{Z}[i]$. Therefore, $\mathbb{Z}[i]$ is closed under addition.

(2) For all $a + bi,\ c + di \in \mathbb{Z}[i]$, we have $(a + bi) \cdot (c + di) = (ac - bd) + (ac + bd)i \in \mathbb{Z}[i]$. Therefore, $\mathbb{Z}[i]$ is closed under multiplication.

(3) $0 = 0 + 0i \in \mathbb{Z}[i]$.

(4) For all $a + bi \in \mathbb{Z}[i]$, we have $(-a) + (-b)i \in \mathbb{Z}[i]$ and $(a + bi) + ((-a) + (-b)i) = 0$.

Therefore, by Theorem 3.2, $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$.

22 Define a new addition $\oplus$ and multiplication $\odot$ on $\mathbb{Z}$ by

$$a \oplus b = a + b - 1 \text{ and } a \odot b = a + b - ab,$$

where the operation on the right-hand side of the equal signs are ordinary addition, subtraction, and multiplication. Prove that, with the new operations $\oplus$ and $\odot$, $\mathbb{Z}$ is an integral domain.

Solution:

Let R denote the set $\mathbb{Z}$ equipped with the above operations $\oplus$ and $\odot$. We have

1. For all $a, b \in R$, $a \oplus b = a + b - 1 \in R$.
2. For all $a, b, c \in R$,
$$a \oplus (b \oplus c) = a \oplus (b + c - 1) = a + (b + c - 1) - 1 = (a + b - 1) + c - 1 = (a \oplus b) \oplus c.$$
3. For all $a, b \in R$, $a \oplus b = a + b - 1 = b + a - 1 = b \oplus a$.
4. Let $0_R = 1 \in \mathbb{Z}$. For all $a \in R$, $a \oplus 0_R = a + 1 - 1 = a = 1 + a - 1 = 0_R \oplus a$.
5. For all $a \in R$, let $x = 2 - a \in \mathbb{R}$. Then $a \oplus x = a + (2 - a) - 1 = 1 = 0_R$.
6. For all $a, b \in R$, we have $a \odot b = a + b - ab \in R$.
7. For all $a, b, c \in R$, we have
$$\begin{aligned} a \odot (b \odot c) &= a \odot (b + c - bc) \\ &= a + (b + c - bc) - a(b + c - bc) \\ &= (a + b + c) - ab - ac - bc + abc \\ &= (a + b - ab) + c - (a + b - ab)c \\ &= (a + b - ab) \odot c \\ &= (a \odot b) \odot c. \end{aligned}$$

8. For all $a, b, c \in R$, we have

$$\begin{aligned} a \odot (b \oplus c) &= a \odot (b + c - 1) \\ &= a + (b + c - 1) - a(b + c - 1) \\ &= (a + b + c) - ab - ac + a - 1 \\ &= (a + b - ab) + (a + c - ac) - 1 \\ &= (a + b - ab) \oplus (a + c - ac) \\ &= (a \odot b) \oplus (a \odot c). \end{aligned}$$

$$\begin{aligned} (a \oplus b) \odot c &= (a + b - 1) \odot c \\ &= (a + b - 1) + c - (a + b - 1)c \\ &= (a + b - 1) + c - ac - bc + c \\ &= (a + c - ac) + (b + c - bc) - 1 \\ &= (a + c - ac) \oplus (b + c - bc) \\ &= (a \odot c) \oplus (b \odot c). \end{aligned}$$

9. For all $a, b \in R$, we have $a \odot b = a + b - ab = b + a - ba = b \odot a$. Therefore, R is commutative.

10. Let $1_R = 0 \in \mathbb{Z}$. Then for all $a \in R$, $a \odot 1_R = a + 0 - a \cdot 0 = a = 0 + a - 0 \cdot a = 1_R \odot a$. Therefore, 1_R is a multiplicative identity of R.

11. Suppose $a, b \in R$ satisfy $a \odot b = 0_R = 1$. We have

$$a + b - ab = 1 \Rightarrow ab - (a + b) + 1 = 0 \Rightarrow (a - 1)(b - 1) = 0 \Rightarrow (a - 1) = 0 \text{ or } (b - 1) = 0$$

We have $(a - 1) = 0 \Rightarrow a = 1 = 0_R$ and $(b - 1) = 0 \Rightarrow b = 1 = 0_R$. Therefore, R is an integral domain.

30. The addition table and part of the multiplication table for a four-element ring are given below. Use the distributive laws to complete the multiplication table.

$+$	w	x	y	z
w	w	x	y	z
x	x	y	z	w
y	y	z	w	x
z	z	w	x	y

and

$\cdot$	w	x	y	z
w	w	w	w	w
x	w	y		
y	w		w	
z	w		w	y

Solution:

By the distributive laws, we have

1. $xy = x(x + x) = xx + xx = y + y = w$
2. $xz = x(x + y) = xx + xy = y + w = y$
3. $yx = (x + x)x = xx + xx = y + y = w$
4. $yz = y(x + y) = yx + yy = w + w = w$

5. $zx = (x+y)x = xx + xy = y + w = y$

Therefore, the complete multiplication table is

$\cdot$	w	x	y	z
w	w	w	w	w
x	w	y	$\mathbf{w}$	$\mathbf{y}$
y	w	$\mathbf{w}$	w	$\mathbf{w}$
z	w	$\mathbf{y}$	w	y

42. A **division ring** is a (not necessarily commutative) ring R with identity $1_R \neq 0_R$ that satisfies Axiom 11 and 12 (pages 48 and 49). Thus a field is a commutative division ring. See Exercise 43 for a noncommutative example. Suppose R is a division ring and a, b are nonzero elements of R.

(a) If $bb = b$, prove that $b = 1_R$. [*Hint:* Let v be a solution of $bx = 1_R$ and note that $bv = b^2v$.]

Solution:

Let v be a solution of $bx = 1_R$. Then $bv = 1_R$. So we have

$$b = b1_R = b(bv) = (bb)v = bv = 1_R.$$

(b) If u is a solution of the equation $ax = 1_R$, prove that u is also a solution of the equation $xa = 1_R$. (Remember that R may not be commutative.) [*Hint:* Use part (a) with $b = ua$.]

Solution:

Let u be a solution of the equation $ax = 1_R$. Then $au = 1_R$. Let $b = ua$. We have

$$b^2 = (ua)(ua) = u(au)a = u1_Ra = ua = b.$$

By the result in part (a), we have $b = 1_R$.

3.2

12. Let a, b be elements of a ring R.

(a) Prove that the equation $a + x = b$ has a unique solution in R. (You must prove that there is a solution *and* that this solution is the only one.)

Solution:

Let $x = (-a) + b$. Then $a + x = a + ((-a) + b) = (a + (-a)) + b = 0_R + b = b$. So $x = (-a) + b$ is a solution of the equation $a + x = b$.

Suppose $y \in R$ satisfies $a + y = b$. Then

$$y = 0_R + y = ((-a) + a) + y = (-a) + (a + y) = (-a) + b = x$$

Therefore, the equation $a + x = b$ has a unique solution $x = (-a) + b$.

(b) If R is a ring with identity and a is a unit, prove that the equation $ax = b$ has a unique solution in R.

Solution:

Suppose a is a unit in R. Then there exists $u \in R$ such that $au = 1_R = ua$. Let $x = ub$. Then

$$ax = a(ub) = (au)b = 1_R b = b.$$

Suppose $y \in R$ such that $ay = b$. Then we have

$$y = 1_R y = (ua)y = u(ay) = ub$$

.

Therefore, the equation $ax = b$ has a unique solution $x = ub$.

18. Let a be a nonzero element of a ring with identity. If the equation $ax = 1_R$ has a solution u and the equation $ya = 1_R$ has a solution v, prove that $u = v$.

Suppose $au = 1_R = va$. Then

$$u = 1_R u = (va)u = v(au) = v1_R = v$$

22.

(a) If ab is a zero divisor in a ring R, prove that a or b is a zero divisor.

Solution:

Suppose ab is a zero divisor in a ring R. Then $ab \neq 0 \Rightarrow a \neq 0$ and $b \neq 0$. Also, there exists a nonzero $c \in R$ such that either (1) $(ab)c = 0$ or (2) $c(ab) = 0$. Consider

(1) $(ab)c = 0$: If $bc = 0$, then b is a zero divisor. If $bc \neq 0$, then $a(bc) = (ab)c = 0$, then a is a zero divisor.

(2) $c(ab) = 0$: If $ca = 0$, then a is a zero divisor. If $ca \neq 0$, then $(ca)b = c(ab) = 0$, then b is a zero divisor.

Thus, in either case, we have a or b is a zero divisor.

(b) If a or b is a zero divisor in a commutative ring R and $ab \neq 0$, prove that ab is a zero divisor.

Solution:

Suppose a or b is a zero divisor in a commutative ring R and $ab \neq 0$.

First consider the case when a is a zero divisor. Then there exists a nonzero $c \in R$ such that $ac = 0 = ca$. Therefore, $c(ab) = (ca)b = 0b = 0$ and (ab) is a zero divisor.

Since R is commutative, the case when b is a zero divisor is similar.

33. Let R be a ring with identity. If ab and a are units in R. Prove that b is a unit.

Solution:

Suppose ab and a are units in R. Then there exist u and v in R such that

$$(ab)u = 1_R = u(ab) \quad \text{and} \quad av = 1_R = va.$$

So we have $(ua)b = u(ab) = 1_R$ and

$$b(ua) = 1_R b(ua) = (va)b(ua) = v(abu)a = v1_R a = va = 1_R$$

Therefore, b is a unit.

40. An element a of a ring is **nilpotent** if $a^n = 0_R$ for some positive integer n. Prove that R has no nonzero nilpotent elements if and only if 0_R is the unique solution of equation $x^2 = 0_R$.

Solution:

Suppose R has no nonzero nilpotent elements. Clearly 0_R satisfies the equation $x^2 = 0_R$. Suppose $a^2 = 0_R$. Then a is nilpotent. Thus, $x = 0_R$. Hence, 0_R is the unique solution of equation $x^2 = 0_R$.

Conversely, suppose 0_R is the unique solution of the equation $x^2 = 0_R$. We are going to prove that R has no nonzero nilpotent elements.

Assume the contrary that there exists a nonzero nilpotent element a in R. Then $a^n = 0_R$ for some $n > 0$. Let $S = \{n | n > 0 \text{ and } a^n = 0_R\} \neq \varnothing$. By the Well Ordering Axiom, S has a smallest element m. Since $a \neq 0_R$ and $a^2 \neq 0_R$, we have $m > 2$. Then we have $a^m = 0_R$ and $m - 2 > 0$. We have

$$\left(a^{m-1}\right)^2 = a^{2m-2} = a^m a^{m-2} = 0_R a^{m-2} = 0_R.$$

Thus a^{m-1} is a solution of the equation $x^2 = 0_R$. Therefore, $a^{m-1} = 0_R \Rightarrow m - 1 \in S$. Since $m - 1 < m$, we have a contradiction.

Hence, R has no nonzero nilpotent elements.