Homework #1 Solutions

p 241, #2 The identity element is easily seen to be 6. Indeed, in $\mathbb{Z}_{10}$ we have

$$\begin{aligned} 2 \cdot 6 &= 12 = 2 \\ 4 \cdot 6 &= 24 = 4 \\ 6 \cdot 6 &= 36 = 6 \\ 8 \cdot 6 &= 48 = 8. \end{aligned}$$

p 241, #4 There are many possible examples. Probably the simplest occurs in $\mathbb{Z}_4$, where both 1 and 3 are solutions to $2x = 2$. We know that such a situation cannot happen in a group, for in that case the equation $ax = b$ has the *unique* solution $x = a^{-1}b$.

p 241, #14 We prove the result for all nonnegative m first. If $m = 0$ the result is obvious. Now assume that $m \geq 1$. Then

$$m \cdot (ab) = \underbrace{ab + ab + \cdots + ab}_{m \text{ times}} = \underbrace{(a + a + \cdots + a)}_{m \text{ times}} b = (m \cdot a)b.$$

If we had instead factored a out on the right side, we would have obtained instead $m \cdot (ab) = a(m \cdot b)$. Thus, $m \cdot (ab) = (m \cdot a)b = a(m \cdot b)$ for all $m \in \mathbb{Z}_0^+$. If $m < 0$ then $m = -n$ for some $n > 0$. We then have, using part 2 of Theorem 12.1 and the preceding result

$$m \cdot (ab) = (-n) \cdot (ab) = n \cdot (-(ab)) = n \cdot ((-a)b) = (n \cdot (-a))b = ((-n) \cdot a)b = (m \cdot a)b.$$

That $m \cdot (ab) = a(m \cdot b)$ as well is proven in a similar fashion. We therefore conclude that $m \cdot (ab) = (m \cdot a)b = a(m \cdot b)$ for all negative integers m as well.

p 242, #22 The multiplication operation in R is associative by definition, the identity 1 of R is a unit $(1 \cdot 1 = 1)$ and clearly functions as the identity in $U(R)$, and the inverse of any unit a is also a unit $(a \cdot a^{-1} = 1)$ which functions as the group inverse in $U(R)$. So we need only show that $U(R)$ is closed under multiplication. So, let $a, b \in U(R)$. Then both a^{-1} and b^{-1} exist in R. Using the same trick we learned for groups, we see that

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a \cdot 1 \cdot a^{-1} = aa^{-1} = 1$$

which proves that $b^{-1}a^{-1}$ is the inverse of ab (we only need to check inverses on one side since R is commutative), i.e. that $ab \in U(R)$. This proves closure and hence that $U(R)$ is a group.

Note: The hypothesis that R is commutative is unnecessary, provided one defines a unit in a (possibly noncommutative) ring with identity to be an element with both a left and a right multiplicative inverse. The proof above is easily modified to apply in this case as well.

p 242, #24 We begin with the following observation. Let $x = (x_1, x_2, \ldots, x_n), y = (y_1, y_2, \ldots, y_n) \in R_1 \oplus R_2 \oplus \ldots \oplus R_n$. Since the identity in the direct sum is $1 = (1, 1, \ldots, 1)$ and multiplication is performed component-wise we see that

$$xy = 1$$

if and only if

$$(x_1 y_1, x_2 y_2, \ldots, x_n y_n) = (1, 1, \ldots, 1)$$

if and only if

$$x_i y_i = 1$$

for $i = 1, 2, \ldots, n$. From this it easily follows that $x \in U(R_1 \oplus R_2 \oplus \cdots \oplus R_n)$ if and only if $x_i \in U(R_i)$ for $i = 1, 2, \ldots, n$, i.e. $x = (x_1, x_2, \ldots, x_n) \in U(R_1) \oplus U(R_2) \oplus \cdots \oplus U(R_n)$. This is precisely the statement that $U(R_1 \oplus R_2 \oplus \cdots \oplus R_n) = U(R_1) \oplus U(R_2) \oplus \cdots \oplus U(R_n)$.

p 242, #28 In $\mathbb{Z}_6$ we have $2 \cdot 4 = 8 = 2$, proving that $4 \,|\, 2$. Likewise, in $\mathbb{Z}_8$, $5 \cdot 3 = 15 = 7$ and in $\mathbb{Z}_{15}$, $3 \cdot 9 = 27 = 12$, proving $3 \,|\, 7$ and $9 \,|\, 12$, respectively.