Ring Theory Problem Set 1 – Solutions

Problem 16.1 Let R be a ring with unity 1. Show that $(-1)a = -a$ for all $a \in R$.

SOLUTION: We have $1+(-1) = 0$ by definition. Multiplying that equation on the right by a, we obtain

$$\big(1+(-1)\big) \cdot a \ = \ 0 \cdot a \ = \ 0$$

by theorem 16.1, part i. By the distributive law, we obtain the equation

$$1 \cdot a + (-1) \cdot a \ = \ 0$$

and therefore we have $a+(-1)a = 0$. We also have $a+(-a) = 0$. Thus, $a+(-1)a = a+(-a)$. The ring R under addition is a group. The cancellation law in that group implies that

$$-a \ = \ (-1)a$$

which is the result we wanted to prove.

Problem 16.7 Let F be a field and let $a,\ b \in F$. Assume that $a \neq 0$, Show that there exists an element $x \in F$ satisfying the equation $ax + b = 0$.

SOLUTION: Since F is a field and $a \neq 0$, there exists an element a^{-1} in F such that $aa^{-1} = 1$. Let $c = -b$. Let $x = a^{-1}c$. Then $x \in F$ since both a^{-1} and c are in F. We have

$$ax + b - = \ a(a^{-1}c) + b \ = \ (aa^{-1})c + b \ = \ 1c + b \ = \ c + b \ = \ 0 \quad .$$

Hence the element x in F chosen above has the property that $ax + b = 0$.

Problem 16.11 Find all units, zero-divisors, and nilpotent elements in the rings $\mathbb{Z} \oplus \mathbb{Z}$, $\mathbb{Z}_3 \oplus \mathbb{Z}_3$, and $\mathbb{Z}_4 \oplus \mathbb{Z}_6$.

SOLUTION; In general, if R_1 and R_2 are rings with unity, then so is $R_1 \oplus R_2$. The unity element is $(1_{R_1},\ 1_{R_2})$. An element $(a_1,\ a_2)$ in $R_1 \oplus R_2$ is a unit if and only if there is an element $(b_1,\ b_2)$ in $R_1 \oplus R_2$ such that $(a_1,\ a_2)(b_1,\ b_2) = (1_{R_1},\ 1_{R_2})$. By definition, $(a_1,\ a_2)(b_1,\ b_2) = (a_1b_1,\ a_2b_2)$. Therefore, the element $(a_1,\ a_2)$ is a unit if and only if there exists elements $b_1 \in R_1$ and $b_2 \in R_2$ such that $a_1b_1 = 1_{R_1}$ and $a_2b_2 = 1_{R_2}$. This means that $(a_1,\ a_2)$ is a unit in $R_1 \oplus R_2$ if and only if a_1 is a unit in R_1 and a_2 is a unit in R_2.

The units in $\mathbb{Z}$ are 1 and -1. The units in $\mathbb{Z}_3$ are 1 and 2. The units in $\mathbb{Z}_4$ are 1 and 3. The units in $\mathbb{Z}_6$ are 1 and 5. Therefore,

The units in $\mathbb{Z} \oplus \mathbb{Z}$ are $(1,1),\ (1,-1),\ (-1,1)$, and $(-1,-1)$.

The units in $\mathbb{Z}_3 \oplus \mathbb{Z}_3$ are $(1,1),\ (1,2),\ (2,1)$, and $(2,2)$.

The units in $\mathbb{Z}_4 \oplus \mathbb{Z}_6$ are $(1,1),\ (1,5),\ (3,1)$, and $(3,5)$.

Suppose that $(a_1,\ a_2)$ is an element of $R_1 \oplus R_2$ and that n is a positive integer. Then we clearly have $(a_1,\ a_2)^n = (a_1^n,\ a_2^n)$. The additive identity in $R_1 \oplus R_2$ is $(0_{R_1},\ 0_{R_2})$. The equation $(a_1,\ a_2)^n = (0_{R_1},\ 0_{R_2})$ is equivalent to the two equations $a_1^n = 0_{R_1}$ and $a_2^n = 0_{R_2}$.

Consequently, if $(a_1,\ a_2)$ is a nilpotent element of $R_1 \oplus R_2$, then it follows that a_1 is a nilpotent element in R_1 and a_2 is a nilpotent element in R_2. The converse is true too. To see this, assume that a_1 is a nilpotent element in R_1 and a_2 is a nilpotent element in R_2. Then, by definition, there exists positive integers e and f such that $a_1^e = 0_{R_1}$ and $a_2^f = 0_{R_2}$. Let $n = ef = fe$. Then n is a positive integer and we have

$$a_1^n = a_1^{ef} = (a_1^e)^f = 0_{R_1}^f = 0_{R_1} \qquad and \qquad a_2^n = a_2^{fe} = (a_2^f)^e = 0_{R_2}^e = 0_{R_2}$$

Therefore, $(a_1,\ a_2)^n = (0_{R_1},\ 0_{R_2})$ and hence $(a_1,\ a_2)$ is a nilpotent element of $R_1 \oplus R_2$. In summary, we have shown that $(a_1,\ a_2)$ is a nilpotent element of $R_1 \oplus R_2$ if and only if a_1 is a nilpotent element in R_1 and a_2 is a nilpotent element in R_2.

The only nilpotent element of $\mathbb{Z}$ is 0. The only nilpotent element of $\mathbb{Z}_3$ is 0. The nilpotent elements of $\mathbb{Z}_4$ are 0 and 2. The only nilpotent element of $\mathbb{Z}_6$ is 0. It follows that

The only nilpotent element in $\mathbb{Z} \oplus \mathbb{Z}$ is $(0,0)$. The only nilpotent element in $\mathbb{Z}_3 \oplus \mathbb{Z}_3$ is $(0,0)$.

The nilpotent elements in $\mathbb{Z}_4 \oplus \mathbb{Z}_6$ are $(0,0)$ and $(2,0)$.

Suppose that $(a_1,\ a_2)$ is an element of $R_1 \oplus R_2$. Then $(a_1,\ a_2)$ is a zero-divisor if and only if there exists an element $(b_1,\ b_2)$ in $R_1 \oplus R_2$ such that

$$(b_1,\ b_2) \neq (0_{R_1},\ 0_{R_2}) \qquad and \qquad (a_1,\ a_2)(b_1,\ b_2) = (0_{R_1},\ 0_{R_2}) \ .$$

The second equation just means that $a_1 b_1 = 0_{R_1}$ and $a_2 b_2 = 0_{R_2}$. Also, $(b_1,\ b_2) \neq (0_{R_1},\ 0_{R_2})$ means that $b_1 \neq 0_{R_1}$ or $b_2 \neq 0_{R_2}$. Consequently, it follows that if $(a_1,\ a_2)$ is a zero-divisor in $R_1 \oplus R_2$, then either a_1 is a zero divisor in R_1 or a_2 is a zero divisor in R_2. For the converse, suppose that a_1 is a zero-divisor in R_1. Then $a_1 b_1 = 0_{R_1}$ for some nonzero element $b_1 \in R_1$. It follows that

$$(b_1,\ 0_{R_2}) \neq (0_{R_1},\ 0_{R_2}) \qquad and \qquad (a_1,\ a_2)(b_1,\ 0_{R_2}) = (0_{R_1},\ 0_{R_2}) \ .$$

Therefore, $(a_1,\ a_2)$ is a zero-divisor in $R_1 \oplus R_2$. A similar argument shows that if a_2 is a zero-divisor in R_2, then $(a_1,\ a_2)$ is a zero-divisor in $R_1 \oplus R_2$. In summary, we have shown that $(a_1,\ a_2)$ is a zero-divisor in $R_1 \oplus R_2$ if and only if either a_1 is a zero divisor in R_1 or a_2 is a zero divisor in R_2.

The only zero-divisor in $\mathbb{Z}$ is 0. The only zero-divisor in $\mathbb{Z}_3$ is 0. The zero-divisors in $\mathbb{Z}_4$ are 0 and 2. The zero-divisors in $\mathbb{Z}_6$ are 0, 2, 3 and 4. The above remark shows that

The set of zero-divisors in $\mathbb{Z} \oplus \mathbb{Z}$ is $\{\ (a,\ 0) \bigm| a \in \mathbb{Z}\ \} \ \cup\ \{\ (0,\ b) \bigm| b \in \mathbb{Z}\ \}$.

The set of zero-divisors in $\mathbb{Z}_3 \oplus \mathbb{Z}_3$ is $\{\ (a,\ 0) \bigm| a \in \mathbb{Z}_3\ \} \ \cup\ \{\ (0,\ b) \bigm| b \in \mathbb{Z}_3\ \}$.

The set of zero-divisors in $\mathbb{Z}_4 \oplus \mathbb{Z}_6$ is

$$\{\ (a,\ b) \bigm| a \in \mathbb{Z}_4,\ b = 0, 2, 3,\ or\ 4\ \} \ \cup\ \{\ (a,\ b) \bigm| b \in \mathbb{Z}_6,\ a = 0\ or\ 2.\} \quad .$$

Problem 16.13, part (a) Show that the multiplicative identity in a ring with unity R is unique.

SOLUTION: Suppose that $e \in R$ and that $ea = a = ae$ for all $a \in R$. Suppose also that $f \in R$ and that $fa = a = af$ for all $a \in R$. Then we have

$$f \ = \ ef \ = \ e$$

Therefore, $e = f$. Thus, there can only be one element in R satisfying the requirements for the multiplicative identity of the ring R.

Problem 16.13, part (b) Suppose that R is a ring with unity and that $a \in R$ is a unit of R. Show that the multiplicative inverse of a is unique.

SOLUTION: Suppose that $b,\ c \in R$ and that $ab = ba = 1$ and that $ac = ca = 1$. Then we have

$$c \ = \ 1c \ = \ (ba)c \ = \ b(ac) \ = \ b1 \ = \ b \ .$$

Hence we have $c = b$. The multiplicative inverse of a is indeed unique.

ADDITIONAL PROBLEMS:

A: Prove that if R is a division ring, then the center of R is a field.

SOLUTION: First of all, suppose that R is any ring with identity. Let S be the center of R. That is,

$$S \; = \; \{ \; s \in R \mid sr = rs \text{ for all } r \in R \; \} \quad .$$

We will show that S is a subring of R.

The fact that S is a subgroup of R under addition can be seen as follows. For this purpose, suppose that $s_1, \; s_2 \in S$. Then, for all $r \in R$, we have $s_1 r = r s_1$ and $s_2 r = r s_2$. Therefore, using the distributive laws for R, we have

$$(s_1 + s_2) r \; = \; s_1 r + s_2 r \; = \; r s_1 + r s_2 \; = \; r(s_1 + s_2)$$

for all $r \in R$. Therefore, $s_1 + s_2 \in S$. Furthermore, letting 0 denote the additive identity of R, we have $0 \cdot r = 0$ and $r \cdot 0 = 0$. Hence $0 \cdot r = r \cdot 0$. Therefore, $0 \in S$.

Finally, suppose that $s \in S$. Let $t = -s$, the additive inverse of s in R. We have $s + t = 0$. Thus, $s + t \in S$. Since s is in S and $s + t$ is in S, it follows that, for all $r \in R$, we have $sr = rs$ and $(s + t)r = r(s + t)$. Therefore, we have

$$sr + tr \; = \; rs + rt \; = \; sr + rt$$

Thus, we have the equation $sr + tr = sr + rt$. Applying the cancellation law for the underlying additive group of R to that equation, it follows that $tr = rt$ for all $r \in R$. Therefore, $t \in S$. That is, $-s \in S$. This completes the verification that S is a subgroup of R under the operation of addition.

To complete the proof that S is a subring of R, we must show that if s_1 and s_2 are in S, then so is $s_1 s_2$. So, assume that $s_1, \; s_2 \in S$. Then, for all $r \in R$, we have $s_1 r = r s_1$ and $s_2 r = r s_2$. Consider $s_1 s_2$, which is an element of R. Using the associative law for multiplication in R many times, it follows that

$$(s_1 s_2) r \; = \; s_1 (s_2 r) \; = \; s_1 (r s_2) \; = \; (s_1 r) s_2 \; = \; (r s_1) s_2 \; = \; r(s_1 s_2)$$

for all $r \in R$. Therefore, we indeed have $s_1 s_2 \in S$.

We have shown that S is a subring of R.

If R is a ring with unity 1, then $1r = r = r1$ for all $r \in R$. Therefore $1 \in S$. Hence S is a ring with unity.

Now we assume that R is a division ring. Then, by definition, R is a ring with unity 1, $1 \neq 0$, and every nonzero element of R is a unit of R. Suppose that S is the center of R. Then, as pointed out above, $1 \in S$ and hence S is a ring with unity. Also, 0 is the additive identity of R and is also the additive identity of the ring S. We have $1 \neq 0$. We now prove that S is a division ring. It suffices to prove that $U(S) = S - \{0\}$. For this purpose, assume that $s \in S$ and $s \neq 0$. Since $s \in U(R)$, there exists an element $t \in R$ such that $st = 1$ and $ts = 1$. Since $s \in S$, we have $sr = rs$ for all $r \in R$. We also have the implications

$$sr = rs \implies t(sr) = t(rs) \implies (ts)r = (tr)s \implies 1r = (tr)s \implies r = (tr)s$$

$$\implies rt = \big((tr)s\big)t \implies rt = (tr)(st) \implies rt = (tr) \cdot 1 \implies rt = tr \quad .$$

Thus, if we assume that $s \in S$, then $tr = rt$ for all $r \in R$. Therefore, $t \in S$. We have proved that if s is a nonzero element of S, then there exists an element $t \in S$ such that $st = 1$ and $ts = 1$. Hence S is a division ring.

Finally, if $a \in S$, then $ar = ra$ for all $r \in R$. Since $S \subseteq R$, we can say that $ab = ba$ for all $b \in S$. Hence S is a commutative ring. Since S has been proved to be a division ring, it follows that S is a field. We have proved that if R is a division ring, then the center of R is a field.

B: Show that $\mathbb{Z} \times \mathbb{Z}$ is not an integral domain.

SOLUTION: Let $R = \mathbb{Z} \times \mathbb{Z}$, the direct product of the ring $\mathbb{Z}$ with itself. The additive identity element of R is $(0, 0)$. Suppose that $a = (1, 0)$ and $b = (0, 1)$. Then a and b are elements of R, and neither is equal to the additive identity element $0_R = (0, 0)$. However, $ab = (1, 0)(0, 1) = (0, 0) = 0_R$. Hence a and b are zero-divisors in the ring R. Thus, the implication $ab = 0_R \Longrightarrow a = 0_R$ *or* $b = 0_R$ is not satisfied by the ring R. The above choice of a and b is a counterexample. This implies that R is not an integral domain.

C: Let $R = \mathbb{Z}_{10}$. We know that R is a commutative ring with unity. Show that R is not an integral domain. Let $S = \{0,\ 2,\ 4,\ 6,\ 8\}$. Show that S is an integral domain. Show that S is a field.

SOLUTION: The fact that R is not an integral domain follows by observing that $2 \cdot 5 = 0$ in the ring R. The elements 2 and 5 are nonzero elements of R, but their product is 0.

Now we consider $S = \{0,\ 2,\ 4,\ 6,\ 8\}$. The fact that S is a subring of R is rather obvious. Under addition, S is just the cyclic subgroup of R generated by the element 2. Hence S is indeed a subgroup of R. It remains to point out that S is closed under multiplication. Note that if $a,\ b \in \mathbb{Z}$ are even, then so is ab. But 10 is also even. Hence $ab + 10k$ is even for all $k \in \mathbb{Z}$. In particular, the remainder that ab gives when divided by 10 must be even. This shows that the set S is indeed closed under multiplication.

The ring S is obviously commutative. Also, the ring S has a multiplicative identity, namely the element 6. . This is verified by noticing that

$$6 \cdot 0 = 0, \qquad 6 \cdot 2 = 2, \qquad 6 \cdot 4 = 4, \qquad 6 \cdot 6 = 6, \qquad 6 \cdot 8 = 8 \qquad .$$

Thus, we have $1_S = 6$. Note that $0_S = 0$ and hence $1_S \neq 0_S$. We can verify that S is a field by showing that the four nonzero elements of S are all invertible. Indeed we have:

$$2 \cdot 8 = 6, \qquad 4 \cdot 4 = 6, \qquad 6 \cdot 6 = 6, \qquad 8 \cdot 2 = 6 \quad .$$

To verify that S is an integral domain, we make the useful observation that every field is an integral domain. To see this, suppose that F is a field. Then F is a commutative ring with unity 1_F and $1_F \neq 0_F$. Furthermore, every nonzero element of F is invertible. Now suppose that a and b are nonzero elements. Then a and b are units in F. Thus, $a,\ b \in U(F)$. As proved in class, it follows that $ab \in U(F)$. But $0_F \notin U(F)$ because $0_F \cdot c = 0_F$ for all $c \in F$ and hence $0_F \cdot c \neq 1_F$ for all $c \in F$. We have proved that if a and b are nonzero elements of F, then ab is also a nonzero element of F. Therefore, F is indeed an integral domain.

Since S is a field, the above useful observation implies that S is also an integral domain.

D: Determine the center of the ring $M_2(\mathbb{R})$.

SOLUTION: To determine the center of the ring $M_2(\mathbb{R})$, we will first find all 2×2 matrices with real entries that commute with the matrix

$$E_{11} \;=\; \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} .$$

We have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \;=\; \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;=\; \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$$

A necessary and sufficient condition for these two products to be equal is that $b = c = 0$. Thus, the set of 2×2 matrices that commute with E_{11} is

$$\left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \;\middle|\; a, d \in \mathbf{R} \right\}$$

Now suppose that A is an element of the center of the ring $M_2(\mathbb{R})$. Then $AB = BA$ for all $B \in M_2(\mathbb{R})$. In particular, we have $AE_{11} = E_{11}A$ and $AE_{21} = E_{21}A$, where

$$E_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

As shown above, the fact that $AE_{11} = E_{11}A$ implies that A has the form

$$A = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$$

where $a, d \in \mathbb{R}$. Now we use the fact that $AE_{21} = E_{21}A$. We have

$$AE_{21} = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ d & 0 \end{pmatrix}, \qquad E_{21}A = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ a & 0 \end{pmatrix}$$

We have $AE_{21} = E_{21}A$ if and only if $a = d$. Thus,

$$A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = aI_2,$$

where $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, a scalar multiple of the identity matrix I_2. Note that I_2 is the multiplicative identity element in the ring $M_2(\mathbb{R})$. It is obvious that matrices of the form aI_2 do indeed commute with all elements of $M_2(\mathbb{R})$. Thus,

$$\{A \in M_2(\mathbb{R}) \mid AB = BA \textit{ for all } B \in M_2(\mathbb{R})\ \} = \{aI_2 \mid a \in \mathbb{R}\ \}$$

That is, the center of the ring $M_2(\mathbb{R})$ is the subring $\{aI_2 \mid a \in \mathbb{R}\ \}$.

E: Consider the following set of matrices:

$$S = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{R} \right\}.$$

Show that S is a subring of $M_2(\mathbb{R})$ and that $S \cong \mathbb{C}$.

SOLUTION: We first prove that the subset

$$S = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{R} \right\}.$$

is a subring of $M_2(\mathbb{R})$. We will then show that $S \cong \mathbb{C}$.

The additive identity element of $M_2(\mathbb{R})$ is $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ and this is clearly in S. For every element $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ in S, its additive inverse is

$$-A \;=\; \begin{pmatrix} -a & -b \\ -(-b) & -a \end{pmatrix} \;,$$

which is indeed in S. Furthermore, suppose that A' is also in S. Then we can write $A' = \begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix}$, where $a', b' \in \mathbb{R}$. Hence

$$A + A' \;=\; \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix} \;=\; \begin{pmatrix} a+a' & b+b' \\ -(b+b') & a+a' \end{pmatrix} \;,$$

which is in S. We have proved that S is a subgroup of the underlying additive group of the ring $M_2(\mathbb{R})$.

To complete the verification that S is a subring of $M_2(\mathbb{R})$, it suffices to show that S is closed under the multiplication operation in $M_2(\mathbb{R})$. Let A and A' be as in the previous paragraph. Then

$$AA' \;=\; \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix} \;=\; \begin{pmatrix} aa' - bb' & ab' + ba' \\ -ba' + a(-b') & -bb' + aa' \end{pmatrix} \;=\; \begin{pmatrix} aa' - bb' & ab' + ba' \\ -(ab' + ba') & aa' - bb' \end{pmatrix} \;,$$

which is indeed in the subset S. We have proved that S is a subring of $M_2(\mathbb{R})$.

Now define a map ϕ from $\mathbb{C}$ to S as follows.: For all $a, b \in \mathbb{R}$, define

$$\phi(a + bi) \;=\; \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

The map ϕ is clearly a bijection from $\mathbb{C}$ to S. We will prove that ϕ is a ring homomorphism and therefore that the subring S of $M_2(\mathbf{R})$ is isomorphic to $\mathbf{C}$.

Consider $z = a + bi,\; w = c + di \in \mathbf{C}$. We have

$$z + w \;=\; (a + c) + (b + d)i, \qquad zw = (ac - bd) + (ad + bc)i$$

and so

$$\phi(z + w) \;=\; \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix} \;=\; \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \;+\; \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \;=\; \phi(z) \;+\; \phi(w)$$

and

$$\begin{aligned}\phi(z)\phi(w) &= \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -bc-ad & -bd+ac \end{pmatrix} \\ &= \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix} = \phi(zw) \ ,\end{aligned}$$

showing that ϕ is indeed a ring homomorphism. Since ϕ is also a bijection, φ is an isomorphism of the ring $\mathbb{C}$ to the ring S.