UH - Math 3330 - Dr. Heier - Spring 2014
HW 11 - Solutions to *Selected* Homework Problems
by Angelynn Alvarez

1. (Section 5.1, Problem 22) Let R be a ring with unity and S be the set of all units in R.

(a) Prove or disprove that A is a subring of R.
(b) Prove or disprove that S is a group with respect to multiplication in R.

Solution.
(a) This statement is false. For example, take the ring $(\mathbb{Z}, +, \cdot)$. The ring of units is $S = \{1, -1\}$—but $-1 + 1 = 0 \notin S$. Thus, S is not closed under addition and is not a subring.

(b) This statement is true.

Proof. Let R be a ring with unity, 1. Let $a, b \in S$. This means that there exist $c, d \in R$ such that $ac = 1$ and $bd = 1$. Then

$$(ab)(dc) = a(bd)c = a(1)(c) = (ac) = 1$$

Thus, $(ab) \in S$ and S is closed under multiplication. Notice that multiplication in S is associative because $\forall\ a, b, c \in S$, $(ab)c = a(bc)$. The identity element is 1. Lastly, by definition of S, each a in S has a multiplicative inverse. Hence, S is a group with respect to multiplication in R. $\square$

2. (Section 5.1, Problem 39a,c) Decide whether each of the following sets S is a subring of the ring $M_2(\mathbb{Z})$. If a set is not a subring, give a reason why it is not. If it is a subring, determine if S is commutative and find the unity, if one exists. For those that have a unity, which elements in S have multiplicative inverses in S?

$$\textbf{(a)}\ S = \left\{ \begin{bmatrix} x & 0 \\ x & 0 \end{bmatrix} \,\middle|\, x \in \mathbb{Z} \right\}, \qquad \textbf{(c)}\ S = \left\{ \begin{bmatrix} x & y \\ x & y \end{bmatrix} \,\middle|\, x \in \mathbb{Z} \right\}$$

Solution.
(a) Note that S is nonempty because $\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$ is in S. Also, if $A = \begin{bmatrix} x & 0 \\ x & 0 \end{bmatrix}$ and $B = \begin{bmatrix} y & 0 \\ y & 0 \end{bmatrix}$ are in S, then

$$A - B = \begin{bmatrix} x-y & 0 \\ x-y & 0 \end{bmatrix} \in S, \text{ and } AB = \begin{bmatrix} xy & 0 \\ xy & 0 \end{bmatrix} \in S$$

So by Theorem 5.4, S is subring. Direct computation shows that this subring is also commutative. S has unity $\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \in S$. Because S has entries in $\mathbb{Z}$, the elements in S which have multiplicative inverses are $\begin{bmatrix} \pm 1 & 0 \\ \pm 1 & 0 \end{bmatrix}$.

(c) Note that S is nonempty because $\begin{bmatrix} 1 & 2 \\ 1 & 2 \end{bmatrix}$ is in S. Also, if $A = \begin{bmatrix} x & y \\ x & y \end{bmatrix}$ and $B = \begin{bmatrix} u & v \\ u & v \end{bmatrix}$ are in S, then

$$A - B = \begin{bmatrix} x-u & y-v \\ x-u & y-v \end{bmatrix} \in S, \text{ and } AB = \begin{bmatrix} xu+yu & xv+yv \\ xu+yu & xv+yv \end{bmatrix} \in S$$

So by Theorem 5.4, S is subring. Direct computation shows that this subring is **not** commutative. Also, S has no unity because $\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \notin S$.

5. (Section 5.2, Problem 3) Consider the set

$$S = \{[0], [2], [4], [6], [8], [10], [12], [14], [16]\} \subseteq \mathbb{Z}_{18}$$

with addition and multiplication as defined in $\mathbb{Z}_{18}$.

(a) Is S an integral domain? If not, give a reason..
(b) Is S a field? If not, give a reason.

Solution.
(a) First note that S is a commutative ring with unity, $[10]$. But $[6][12] = [72] = [0]$ in $\mathbb{Z}_{18}$. So $[6]$ and $[12]$ are zero divisors. Thus, S is not an integral domain.

(b) There does not exist an element $[x] \in S$ such that $[6][x] = [10]$, or $[12][x] = [10]$. So not every element in S has a multiplicative inverse and S is not a field.

8. (Section 5.2, Problem 11) Let R be the set of all matrices of the form $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$, where a and b are real numbers. Assume that R is a ring with respect to matrix addition and multiplication. Answer the following questions and give reason for any negative answers.

(a) Is R a commutative ring?
(b) Does R have a unity? If so, identity the unity.
(c) Is R an integral domain?
(d) Is R a field?

Solution.
(a) Let $A = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ and $B = \begin{bmatrix} c & -d \\ d & c \end{bmatrix}$ be elements in R. Then

$$AB = \begin{bmatrix} ac - bd & -ad - bc \\ bc + cd & -bd + ac \end{bmatrix} = BA$$

due to multiplication in $\mathbb{R}$ being commutative. Thus, R is a commutative ring.

(b) The unity of R is $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

(c) As shown in parts **(a)** and **(b)**, R is a commutative ring with unity. So, all to check now is if R has zero divisors. Let $A, B \in R$ as above, where $A, B \neq 0$. Then

$$AB = \begin{bmatrix} ac - bd & -ad - bc \\ bc + cd & -bd + ac \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

So R does not have any zero divisors and thus is an integral domain.

(d) All to check now is if every nonzero element in R has a multiplicative inverse. Let $A = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \in R$, where $A \neq 0$. Note that $\det(A) = a^2 + b^2 \neq 0$, since either a or b must be nonzero. Thus, A is invertible, and R is a field.

10. (Section 5.2, Problem 20a) Find the multiplicative inverse of the given element: $[11]$ in $\mathbb{Z}_{317}$.

Solution. Applying the Division Algorithm gives us

$$317 = 11(28) + 9, \quad 11 = 9(1) + 1, \quad 9 = 2(4) + 1$$

Thus,

$$\begin{aligned} 1 &= 9 - 2(4) \\ &= 2 - (11 - 9)(4) \\ &= 9(5) = 11(4) \\ &= [317 - 11(28)]5 - 11(4) \end{aligned}$$

Thus, $1 \equiv -11(144)(\text{mod} 317) \iff 1 \equiv (11)(173)(\text{mod} 317)$. So $[11][173] = [1]$ in $\mathbb{Z}_{317}$, and $\boxed{[11]^{-1} = [173]}$.