Homework #1 (SOLUTIONS)

Math 546 DUE: January 18, 2012

EXERCISES (page 234):

2. The set $\{0, 2, 4, 6, 8\}$ under addition and multiplication modulo 10 has a unity. Find it.
6 is the unity of the given set because $6.2 \equiv_{10} 2$, $6.4 \equiv_{10} 4$, $6.6 \equiv_{10} 6$, $6.8 \equiv_{10} 8$ and the set is commutative under multiplication modulo 10.

14. Let a and b belong to a ring R and let m be an integer. Prove that $m.(ab) = (m.a)b = a(m.b)$.
Proof of $(m.a)b = m.(ab)$:
Case (1): Assume $m > 0$. Then $(m.a)b = (\underbrace{a + a + \ldots + a}_{m})b$ (Notation) $= (\underbrace{ab + ab + \ldots + ab}_{m})$ ((Right Distributive Law) $= m.(ab)$ (Notation). Case (2): Assume $m < 0$. So, there exists $k \in \mathbb{Z}^+$ with $m = -k$. $(m.a)b = ((-k).a)b = (-(ka))b(Notation : (-n)a = n(-a) = -(na)) = -((ka)b))$ (Theorem 12.1:(-a)b=-(ab)) $= -(k.(ab))$ (Case (1)) $= (-k).(ab))$ (Notation) $= = m.(ab)$ (since $m = -k$). Case (3): Assume $m = 0$. In this case $m.(ab) = (m.a)b = a(m.b) = 0$.
Proof of $a(m.b) = m.(ab)$:
Case (1): Assume $m > 0$. Then $a(m.b) = a(\underbrace{b + b + \ldots + b}_{m})$ (Notation) $= (\underbrace{ab + ab + \ldots + ab}_{m})$ ((Right Distributive Law) $= m.(ab)$ (Notation). Case (2): Assume $m < 0$. So, there exists $k \in \mathbb{Z}^+$ with $m = -k$. $a(m.b) = a((-k)b) = a(-(kb))(Notation) = -(a(kb))$ (Theorem 12.1:a(-b)=-(ab)) $= -(k.(ab))$ (Case (1)) $= (-k).(ab))$ (Notation) $= = m.(ab)$ (since $m = -k$). Case (3): Assume $m = 0$. In this case $m.(ab)$ $= a(m.b) = 0$.

22. Let R be a commutative ring with unity and let U(R) denote the set of units of R. Prove that U(R) is a group under the multiplication of R. (This group is called the **group of units** of R.
Verify the 4 axioms of the definition of a group.
Closure: Let $u, v \in$ U(R). Then u^{-1}, $v^{-1} \in$ R. Then $v^{-1}u^{-1} \in$ R, since R is closed under multiplication. Thus $(uv)^{-1} = v^{-1}u^{-1} \in R$. Hence $uv \in$ U(R). Associative Law: Since multiplication is associative on R and U(R) $\subseteq R$, multiplication is associative on U(R). Identity: $1 \in R$ and $1^{-1} = 1 \in R$, $1 \in$U(R). Inverses: Let $u \in$ U(R). Then $u^{-1} \in R$. So $(u^{-1})^{-1} = u \in R$. Hence $u^{-1} \in$ U(R).

38. Let $M_2(\mathbb{Z})$ be the ring of all 2×2 matrices over the integers and let $R = \{\begin{bmatrix} a & a+b \\ a+b & b \end{bmatrix} |a, b \in \mathbb{Z}\}$.
Prove or disprove that R is a subring of $M_2(\mathbb{Z})$.
Apply "Subring Test" to the given set R: (1): $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in R$, since $0 \in \mathbb{Z}$ and $0 + 0 = 0$. (2): Let $\begin{bmatrix} a & a+b \\ a+b & b \end{bmatrix}$ and $\begin{bmatrix} c & c+d \\ c+d & d \end{bmatrix}$ be in R. Then $\begin{bmatrix} a & a+b \\ a+b & b \end{bmatrix}$ - $\begin{bmatrix} c & c+d \\ c+d & d \end{bmatrix}$ = $\begin{bmatrix} a-c & a+b-(c+d) \\ a+b-(c+d) & b-d \end{bmatrix} \in R$. (3): R is not closed under multiplication because, for example, $\begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}$ and $\begin{bmatrix} 2 & 4 \\ 4 & 2 \end{bmatrix} \in R$ but $\begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 2 & 4 \\ 4 & 2 \end{bmatrix} = \begin{bmatrix} 10 & 8 \\ 8 & 10 \end{bmatrix} \notin R$.

40. Let $R = \{\begin{bmatrix} a & a \\ b & b \end{bmatrix} |a, b \in \mathbb{Z}\}$. Prove or disprove that R is a subring of $M_2(\mathbb{Z})$.
Apply "Subring Test" to the given set R:
(1): $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in R$.
Let $\begin{bmatrix} a & a \\ b & b \end{bmatrix}$ and $\begin{bmatrix} c & c \\ d & d \end{bmatrix}$ be in R. Then (2): $\begin{bmatrix} a & a \\ b & b \end{bmatrix}$ - $\begin{bmatrix} c & c \\ d & d \end{bmatrix} = \begin{bmatrix} a-c & a-c \\ b-d & b-d \end{bmatrix} \in R$. (3): $\begin{bmatrix} a & a \\ b & b \end{bmatrix} \begin{bmatrix} c & c \\ d & d \end{bmatrix} \in R = \begin{bmatrix} ac+ad & ac+ad \\ bc+bd & bc+bd \end{bmatrix} \in R$.

42. Suppose there is a positive even integer n such that $a^n = a$ for all elements of some ring. Show that $-a = a$ for all a in the ring.
Let $a \in R$. Show $-a \in R$. Since $-a \in R$, from the condition, $(-a)^n = -a$. Also, there exists a positive integer m such that $n = 2m$ and $(-a)^n = (-a)^{2m} = ((-a)^2)^m = ((-a)(-a))^m$ (Notation) $= (a^2)^m$ (Theorem 12.1 (3)) $= a^{2m}$ (Notation) $= a^n = a$ (given condition). Thus $-a = (-a)^n = a$

44. Show that $2\mathbb{Z} \cup 3\mathbb{Z}$ is not a subring of $\mathbb{Z}$.
$2\mathbb{Z}\cup 3\mathbb{Z}$ is not closed under addition, since $2 \in 2\mathbb{Z} \subseteq 2\mathbb{Z}\cup 3\mathbb{Z}$ and $3 \in 3\mathbb{Z} \subseteq 2\mathbb{Z}\cup 3\mathbb{Z}$ but $2+3 = 5 \notin 2\mathbb{Z}\cup 3\mathbb{Z}$.

48. Suppose that R is a ring such that $a^2 = a$ for all a in R. Show that R is commutative.
Let $a, b \in R$. Show $ab = ba$. Since $a + b \in R$, $(a + b)^2 = a + b$. Also $(a + b)^2 = (a + b)(a + b)$ (Notation) $= a^2 + ab + ba + b^2$ (Distributive Law) $= a + ab + ba + b$ (From the given condition) $= a + b + ab + ba$ (Addition is commutative on R). So $a + b = a + b + ab + ba \implies 0 = ab + ba \implies ba = -(ab)$. Now $ba = (ba)^2$ (Given condition, since $ba \in R$) $= (-(ab))^2$ (From above) $= (ab)^2 = ab$ (Given codition).