Math 236
Fall 2006
Dr. Seelinger

Solution for §3.1

Problem 5: Consider the following sets and determine whether each set is a subring of $M_2(\mathbb{R})$. If a set is a subring of $M_2(\mathbb{R})$, determine whether it has an identity.

(a) Let S be the set of all matrices of the form $\begin{bmatrix} 0 & r \\ 0 & 0 \end{bmatrix}$ where r is a rational number. We claim that S is a subring.

In particular, let $\begin{bmatrix} 0 & r_1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & r_2 \\ 0 & 0 \end{bmatrix} \in S$. Then

$$\begin{bmatrix} 0 & r_1 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & r_2 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & r_1 + r_2 \\ 0 & 0 \end{bmatrix} \in S$$

so S is closed under addition. Next, note that

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in S$$

Since 0 is a rational number. Furthermore,

$$\begin{bmatrix} 0 & r_1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & r_2 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in S$$

so S is closed under multiplication. Finally, note the additive inverse of

$$\begin{bmatrix} 0 & r_1 \\ 0 & 0 \end{bmatrix}$$

is

$$\begin{bmatrix} 0 & -r_1 \\ 0 & 0 \end{bmatrix}$$

which is in S since $-r_1$ is rational. Therefore, S is a subring of $M_2(\mathbb{R})$ by Theorem 3.2.

Next, note that S does not have an identity element since the product of any two elements in S is $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

(b) Let T be the set of all matrices of the form $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ where $a, b, c \in \mathbb{Z}$. We claim that T is a subring.

In particular, let $\begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}, \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix} \in T$. Then

$$\begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix} = \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ 0 & c_1 + c_2 \end{bmatrix} \in T$$

so T is closed under addition. Next,

$$\begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}\begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 & a_1b_2 + b_1c_2 \\ 0 & c_1c_2 \end{bmatrix} \in T$$

so T is closed under multiplication. Furthermore, note that

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in T$$

since we can consider the case when $a_1 = b_1 = c_1 = 0$. Finally, note the additive inverse of

$$\begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}$$

is

$$\begin{bmatrix} -a_1 & -b_1 \\ 0 & -c_1 \end{bmatrix}$$

which is in T since $-a_1, -b_1, -c_1 \in \mathbb{Z}$. Therefore, T is a subring of $M_2(\mathbb{R})$ by Theorem 3.2.

Next, note that the identity element of T is $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

(c) Let W be the set of all matrices of the form $\begin{bmatrix} a & a \\ b & b \end{bmatrix}$ where $a, b \in \mathbb{R}$. We claim that W is a subring.

In particular, let $\begin{bmatrix} a_1 & a_1 \\ b_1 & b_1 \end{bmatrix}, \begin{bmatrix} a_2 & a_2 \\ b_2 & b_2 \end{bmatrix} \in W$. Then

$$\begin{bmatrix} a_1 & a_1 \\ b_1 & b_1 \end{bmatrix} + \begin{bmatrix} a_2 & a_2 \\ b_2 & b_2 \end{bmatrix} = \begin{bmatrix} a_1 + a_2 & a_1 + a_2 \\ b_1 + b_2 & b_1 + b_2 \end{bmatrix} \in W$$

so W is closed under addition. Next,

$$\begin{bmatrix} a_1 & a_1 \\ b_1 & b_1 \end{bmatrix}\begin{bmatrix} a_2 & a_2 \\ b_2 & b_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 + a_1b_2 & a_1a_2 + a_1b_2 \\ b_1a_2 + b_1b_2 & b_1a_2 + b_1b_2 \end{bmatrix} \in W$$

so W is closed under multiplication. Furthermore, note that

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in T$$

since we can consider the case when $a_1 = b_1 = 0$. Finally, note the additive inverse of

$$\begin{bmatrix} a_1 & a_1 \\ b_1 & b_1 \end{bmatrix}$$

is

$$\begin{bmatrix} -a_1 & -a_1 \\ -b_1 & -b_1 \end{bmatrix}$$

which is in W. Therefore, W is a subring of $M_2(\mathbb{R})$ by Theorem 3.2.

Note that W does not have an identity element.

(d) Let X be the set of all matrices of the form $\begin{bmatrix} a & 0 \\ a & 0 \end{bmatrix}$ where $a \in \mathbb{R}$. We claim that X is a subring.

In particular, let $\begin{bmatrix} a_1 & 0 \\ a_1 & 0 \end{bmatrix}, \begin{bmatrix} a_2 & 0 \\ a_2 & 0 \end{bmatrix} \in X$. Then

$$\begin{bmatrix} a_1 & 0 \\ a_1 & 0 \end{bmatrix} + \begin{bmatrix} a_2 & 0 \\ a_2 & 0 \end{bmatrix} = \begin{bmatrix} a_1 + a_2 & 0 \\ a_1 + a_2 & 0 \end{bmatrix} \in X$$

so X is closed under addition. Next,

$$\begin{bmatrix} a_1 & 0 \\ a_1 & 0 \end{bmatrix} \begin{bmatrix} a_2 & 0 \\ a_2 & 0 \end{bmatrix} = \begin{bmatrix} a_1 a_2 & 0 \\ a_1 a_2 & 0 \end{bmatrix} \in X$$

so X is closed under multiplication. Furthermore, note that

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in X$$

since we can consider the case when $a_1 = 0$. Finally, note the additive inverse of

$$\begin{bmatrix} a_1 & 0 \\ a_1 & 0 \end{bmatrix}$$

is

$$\begin{bmatrix} -a_1 & 0 \\ -a_1 & 0 \end{bmatrix}$$

which is in X. Therefore, X is a subring of $M_2(\mathbb{R})$ by Theorem 3.2.

Note that the identity element of X is $\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$.

(e) Let D be the set of all matrices of the form $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ where $a, b \in \mathbb{R}$. We claim that D is a subring.

In particular, let $\begin{bmatrix} a_1 & 0 \\ 0 & b_1 \end{bmatrix}, \begin{bmatrix} a_2 & 0 \\ 0 & b_2 \end{bmatrix} \in D$. Then

$$\begin{bmatrix} a_1 & 0 \\ 0 & b_1 \end{bmatrix} + \begin{bmatrix} a_2 & 0 \\ 0 & b_2 \end{bmatrix} = \begin{bmatrix} a_1 + a_2 & 0 \\ 0 & b_1 + b_2 \end{bmatrix} \in D$$

so D is closed under addition. Next,

$$\begin{bmatrix} a_1 & 0 \\ 0 & b_1 \end{bmatrix} \begin{bmatrix} a_2 & 0 \\ b_2 & 0 \end{bmatrix} = \begin{bmatrix} a_1 a_2 & 0 \\ 0 & b_1 b_2 \end{bmatrix} \in D$$

so D is closed under multiplication. Furthermore, note that

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in D$$

since we can consider the case when $a_1 = b_1 = 0$. Finally, note the additive inverse of

$$\begin{bmatrix} a_1 & 0 \\ 0 & b_1 \end{bmatrix}$$

is

$$\begin{bmatrix} -a_1 & 0 \\ 0 & -b_1 \end{bmatrix}$$

which is in D. Therefore, D is a subring of $M_2(\mathbb{R})$ by Theorem 3.2.

Note that the identity element of D is $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

(f) Let R be the set of all matrices of the form $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$ where $a \in \mathbb{R}$. We claim that R is a subring.

In particular, let $\begin{bmatrix} a_1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} a_2 & 0 \\ 0 & 0 \end{bmatrix} \in D$. Then

$$\begin{bmatrix} a_1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} a_2 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a_1 + a_2 & 0 \\ 0 & 0 \end{bmatrix} \in R$$

so R is closed under addition. Next,

$$\begin{bmatrix} a_1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a_2 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a_1 a_2 & 0 \\ 0 & 0 \end{bmatrix} \in R$$

so R is closed under multiplication. Furthermore, note that

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in R$$

since we can consider the case when $a_1 = 0$. Finally, note the additive inverse of

$$\begin{bmatrix} a_1 & 0 \\ 0 & 0 \end{bmatrix}$$

is

$$\begin{bmatrix} -a_1 & 0 \\ 0 & 0 \end{bmatrix}$$

which is in R. Therefore, R is a subring of $M_2(\mathbb{R})$ by Theorem 3.2.

Note that the identity element of R is $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$.

Problem 9 Let $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\} \subseteq \mathbb{R}$. Prove $\mathbb{Z}[\sqrt{2}]$ is a subring of $\mathbb{R}$.

Proof: Consider $a + b\sqrt{2}, c + d\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ where $a, b, c, d \in \mathbb{Z}$. Then $(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, so $\mathbb{Z}[\sqrt{2}]$ is closed under addition. Also, $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ since $ac+2bd, ad+bc \in \mathbb{Z}$. So $\mathbb{Z}[\sqrt{2}]$ is closed under multiplication. Next, $0 = 0 + 0\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Finally, the additive inverse of $a + b\sqrt{2}$ is $(-a) + (-b)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Therefore, by Theorem 3.2, $\mathbb{Z}[\sqrt{2}]$ is a subring of $\mathbb{R}$. Q.E.D.

Problem 10 Let $\mathbb{Z}[\mathbf{i}] = \{a + b\mathbf{i} : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$. Prove $\mathbb{Z}[\mathbf{i}]$ is a subring of $\mathbb{C}$.

Proof: Consider $a+b\mathbf{i}, c+d\mathbf{i} \in \mathbb{Z}[\mathbf{i}]$ where $a, b, c, d \in \mathbb{Z}$. Then $(a+b\mathbf{i})+(c+d\mathbf{i}) = (a+c)+(b+d)\mathbf{i} \in \mathbb{Z}[\mathbf{i}]$, so $\mathbb{Z}[\mathbf{i}]$ is closed under addition. Also, $(a + b\mathbf{i})(c + d\mathbf{i}) = (ac - bd) + (ad + bc)\mathbf{i} \in \mathbb{Z}[\mathbf{i}]$ since $ac - bd, ad + bc \in \mathbb{Z}$. So $\mathbb{Z}[\mathbf{i}]$ is closed under multiplication. Next, $0 = 0 + 0\mathbf{i} \in \mathbb{Z}[\mathbf{i}]$. Finally, the additive inverse of $a + b\mathbf{i}$ is $(-a) + (-b)\mathbf{i} \in \mathbb{Z}[\mathbf{i}]$. Therefore, by Theorem 3.2, $\mathbb{Z}[\mathbf{i}]$ is a subring of $\mathbb{C}$. Q.E.D.

Problem 18 Define a new addition $\oplus$ and a new multiplication $\otimes$ on $\mathbb{Z}$ by

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

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

To prove this, we need to check the eight conditions in the definition of a ring, then check the additional conditions on being an integral domain. So let $a, b, c \in \mathbb{Z}$.
(1) Since $a, b \in \mathbb{Z}$, we have $a \oplus b = a + b - 1 \in \mathbb{Z}$.
(2) Note $a\oplus(b\oplus c) = a\oplus(b+c-1) = a+(b+c-1)-1 = (a+b-1)+c-1 = (a+b-1)\oplus c = (a\oplus b)\oplus c$. So associativity of addition holds.
(3) We also see $a \oplus b = a + b - 1 = b + a - 1 = b \oplus a$, so commutativity of addition holds.
(4) Note that if we set $\mathcal{O} = 1$ we see that $a \oplus \mathcal{O} = a \oplus 1 = a + 1 - 1 = a$, so $\mathcal{O} = 1$ is the zero element.
(5) Consider the equation $1 = \mathcal{O} = a \oplus x = a + x - 1$. Solving this equation for x gives $x = 2 - a \in \mathbb{Z}$, so this property holds.
(6) Note that $a \otimes b = a + b - ab \in \mathbb{Z}$ since $a, b \in \mathbb{Z}$.
(7) Consider $a\otimes(b\otimes c) = a\otimes(b+c-bc) = a+(b+c-bc)-a(b+c-bc) = a+b+c-ab-bc-ac+abc$ and $(a \otimes b) \otimes c = (a + b - ab) \otimes c = (a + b - ab) + c - (a + b - ab)c = a + b + c - ab - ac - bc + abc$. So $a \otimes (b \otimes c) = (a \otimes b) \otimes c$ and associativity of multiplication holds.
(8) For the distributive property, note $a \otimes (b \oplus c) = a \otimes (b + c - 1) = a + b + c - 1 - a(b + c - 1) = 2a + b + c - ab - ac - 1 = (a + b - ab) + (a + c - ac) - 1 = (a \otimes b) + (a \otimes c) - 1 = (a \otimes b) \oplus (a \otimes c)$ and $(a \oplus b) \otimes c = (a + b - 1) \otimes c = a + b - 1 + c - (a + b - 1)c = a + b + 2c - ac - bc - 1 = (a + c - ab) + (b + c - bc) - 1 = (a \otimes c) + (b \otimes c) - 1 = (a \otimes c) \oplus (b \otimes c)$ so the distributive

properties hold.
(9) Note that $a \otimes b = a + b - ab = b + a - ba = b \otimes a$, so this ring is commutative.
(10) Let $I_R = 0$. Then $a \otimes I_R = a \otimes 0 = a + 0 - a0 = a$ and $I_R \otimes a = 0 \otimes a = 0 + a - 0a = a$, so $I_R = 0$ is the multiplicative identity.

The above shows that $\mathbb{Z}$ with the operations $\oplus$ and $\otimes$ is a commutative ring with identity. Now we need to show that it is also an integral domain. So assume $a \otimes b = \mathcal{O}$. This equation translates to $a + b - ab = 1$. But $a + b - ab = 1 \Rightarrow 0 = ab - a - b + 1 = (a-1)(b-1) \Rightarrow a - 1 = 0$ or $b - 1 = 0 \Rightarrow a = 1 = \mathcal{O}$ or $b = 1 = \mathcal{O}$. Hence this ring is an integral domain. Q.E.D.

Problem 22 Let L be the set of all positive real numbers and for any $a, b \in L$ define $a \oplus b = ab$ and $a \otimes b = a^{\log b}$. (a) Prove that L is a ring under the operations $\oplus$ and $\otimes$. (b) Is L a commutative ring? (c) Is L a field?

(a) We need to demonstrate the eight properties in the definition of a ring. So let $a, b, c \in L$.

(1) Since $a, b \in L$, then $a \oplus b = ab \in L$ as the product of two positive real numbers is a positive real number.

(2) Note $a \oplus (b \oplus c) = a \oplus (bc) = a(bc) = (ab)c = (ab) \oplus c = (a \oplus b) \oplus c$.

(3) Next, $a \oplus b = ab = ba = b \oplus a$.

(4) To get a zero element, we need a number O_L such that $a = a \oplus O_L = aO_L$. Hence $O_L = 1 \in L$ is the zero element.

(5) We need to solve $a \oplus x = O_L = 1$. This translates to $ax = 1$, so $x = (1/a) \in L$ since a is a positive (non-zero) real number.

(6) Now $a \otimes b = a^{\log b}$. But since b is a positive real number, $\log b$ is a real number. Therefore, the positive number a raised to a real exponent $\log b$ is still positive, hence $a^{\log b} \in L$.

(7) Note $a \otimes (b \otimes c) = a \otimes (b^{\log c}) = a^{\log(b^{\log c})} = a^{(\log b)(\log c)} = (a^{\log b})^{\log c} = (a \otimes b)^{\log c} = (a \otimes b) \otimes c$, since $\log(b^{\log c}) = (\log c)(\log b)$ by the properties of logs.

(8) Now $a \otimes (b \oplus c) = a \otimes (bc) = a^{\log(bc)} = a^{\log b + \log c} = a^{\log b} a^{\log c} = (a \otimes b)(a \otimes c) = (a \otimes b) \oplus (a \otimes c)$ and $(a \oplus b) \otimes c = (ab) \otimes c = (ab)^{\log c} = a^{\log c} b^{\log c} = (a \otimes c)(b \otimes c) = (a \otimes c) \oplus (b \otimes c)$.

Therefore, since L satisfies the definition of a ring, L is a ring under the operations $\oplus$ and $\otimes$.

(b) To show L is commutative, we need to show $a \otimes b = b \otimes a$. But $a \otimes b = a^{\log b} = (e^{loga})^{\log b} = e^{(\log a)(\log b)} = e^{(\log b)(\log a)} = (e^{\log b})^{\log a} = b^{\log a} = b \otimes a$. Therefore, L is a commutative ring.

(c) In order for L to be a field, we need to show first that L has an identity, then if $a \neq O_L$, a^{-1} exists. First we show L has an identity, I. So we need to solve $a \otimes I = a$. So $a^{\log I} = a$, which implies $\log I = 1$ when $a \neq O_l = 1$. If $\log I = 1$, then $I = e^1 = e$. Therefore, e is the multiplicative identity.

Now let $a \neq 1 = O_L$ and set $a \otimes x = e = I$. Then $e = a^{\log x} = e^{(\log a)(\log x)}$. So $(\log a)(\log x) = 1$ which gives us that $x = e^{(1/(\log a))} \in L$ when $a \neq 1$. Therefore, every $a \neq 1 = O_L$ in L has a multiplicative inverse $e^{(1/(\log a))}$ so L is a field.