Math 412. Adventure sheet on Ring Basics

DEFINITION: A **ring**[1] is a non-empty set R with two binary operations, denoted "$+$" and "$\times$," such that

- $+$ and $\times$ are both associative,
- $+$ is commutative,
- $+$ has a identity, which we denote 0_R;
- Every element of R has an inverse for the operation $+$; the inverse of r is denoted $-r$.
- $\times$ has an identity, denoted 1_R;
- The two operations are related by the *distributive properties*: $a \times (b + c) = a \times b + a \times c$ and $(a + b) \times c = a \times c + b \times c$ for all $a, b, c \in R$.

A. EXAMPLES OF RINGS. Which of the following have a natural ring structure? Describe the addition, multiplication, and identity elements.

(1) The set of polynomials $\mathbb{R}[x]$ with coefficients in $\mathbb{R}$.
(2) The set $\mathcal{P}_d$ of polynomials in $\mathbb{R}[x]$ of degree at most d.
(3) The set $M_2(\mathbb{R})$ of 2×2 matrices with coefficients in $\mathbb{R}$.
(4) The *Gaussian integers* $\mathbb{Z}[i] = \{a + bi \,|\, a, b \in \mathbb{Z}\}$.
(5) The set $\{even, odd\}$.
(6) The set $\mathbb{Z}_N$ for any positive integer N.
(7) The set of all 2×3 matrices with coefficients in $\mathbb{Z}$.
(8) The set of all 2×2 matrices with coefficients in $\mathbb{R}$ and non-zero determinant.
(9) The set $\mathcal{C}(\mathbb{R})$ of continuous functions from $\mathbb{R}$ to itself.
(10) The set of increasing functions from $\mathbb{R}$ to iself.

(1) Yes! Add and multiply polynomials as usual. The additive identity is the constant polynomial 0 and the multiplicative identity is the constant polynomial 1.
(2) No, at least not with usual polynomial multiplication. Multiplying two polynomials of degree d gives us a polynomials of degree $2d$, which is not in the set.
(3) Yes. The 0 is the zero matrix $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, and the 1 is the constant identity matrix $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.
(4) Yes! Define $(a+bi)+(c+di) = (a+c)+(b+d)i$ and $(a+bi)\cdot(c+di) = (ac-bd)+(ad+bc)i$. The zero is $0 + 0i$ and the one is $1 + 0i$.
(5) Yes! This is the ring $\mathbb{Z}_2$.
(6) Yes! We checked this last week.
(7) No! No natural multiplication, since you can't multiply a 2×3 matrix by a 2×3 matrix.
(8) No, no zero.
(9) Yes, with the usual addition and multiplication from calculus $(f + g)(x) = f(x) + g(x), (fg)(x) = f(x)g(x)$, and identities constant functions zero and one.
(10) No: no additive inverses.

B. EASY PROOFS: Let $\square$ be an operation on a set T.

(1) Prove that $\square$ has at most one identity. Can a ring R have more than one 0_R? What about more than one 1_R? Explain.
(2) Suppose $\square$ is associative. Prove that the $\square$-inverse of any element $x \in T$, if it exists, is unique. Can elements of rings have more than one additive/multiplicative inverses?
(3) Prove that in any ring R, $0_R \times x = 0_R$ for all $x \in R$.[2]

[1] WARNING: Our definition requires that a ring have a multiplicative identity. The is different from the book's.

[2] Hint: Use the distributive law with lots of 0's.

(4) TRUE OR FALSE: In any ring R, $(a+b)^2 = a^2 + 2ab + b^2$ for all $a, b \in R$.

(1) Suppose e_1 and e_2 are identities. Then $e_1 \Box_2 = e_1$ (because e_2 is an identity) and also $e_1 \Box e_2 = e_2$ (because e_1 is an identity). So $e_1 = e_2$. QED As a corollary, we deduce that both 0_R and 1_R are unique in any ring R.

(2) Suppose that x and y are $\Box$-inverses of r. Then $x \Box r = e$, where e is the $\Box$-identity. Apply $\Box\ y$ (on the right) to both sides: $(x \Box r) \Box y = e \Box y$. By associativity and definition of e: $x \Box (r \Box y) = y$. But now because y is an additive inverse of r, we have $x \Box e = y$ so $x = y$.

(3) $0 \cdot x = (0+0) \cdot x = 0 \cdot x + 0 \cdot x$. Now, we can add the additive inverse of the element $0 \cdot x$ from both sides. This gives $0 = 0 \cdot x$, as needed.

(4) FALSE: The statement holds if and only if $ab = ba$. There are non-commutative rings, so the statement is not true in general. For example, in $M_2(\mathbb{R})$, take $a = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, b = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.

C. PRODUCT RINGS. Let R and S be rings.[3] Let $R \times S$ be the set of ordered pairs $\{(r, s) \mid r \in R, s \in S\}$.

(1) Define an operation called $+$ on $R \times S$ by $(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$. The three different plus signs in the preceding sentence have three different meanings; explain.

(2) Is this operation on $R \times S$ is associative and commutative? Does it have an identity? Does every $(r, s) \in R \times S$ have an inverse under $+$?

(3) Define a natural multiplication on $R \times S$ so that, together with the addition defined in (1), the set $R \times S$ becomes a ring.

(4) How many elements are in the ring $\mathbb{Z}_N \times \mathbb{Z}_M$?

(5) Make tables for the addition and multiplication in $\mathbb{Z}_2 \times \mathbb{Z}_2$. Identify the multiplicative and additive identity elements. Which elements have a multiplicative inverse?

(1) There three +'s are the three different additions: one in R, one in S and one in $R \times S$.

(2) Yes, See this follows directly from the definition, with $(0_R, 0_S)$ as the identity. See also Theorem 3.1 in the book.

(3) Define multiplication by $(r_1, s_1) \cdot (r_2, s_2) = (r_1 \cdot r_2, s_1 \cdot_2)$. It is associative and has identity $(1_R, 1_S)$, which follows directly from the definition.

(4) NM

(5) $\mathbb{Z}_2 \times \mathbb{Z}_2$ has four elements $(0,0), (1,0), (0,1)$ and $(1,1)$. The zero is $(0,0)$ and the 1 is $(1,1)$.

$+$	(0, 0)	(1, 1)	(1, 0)	(0, 1)
(0, 0)	(0, 0)	(1, 1)	(1, 0)	(0, 1)
(1, 1)	(1, 1)	(0, 0)	(0, 1)	(1, 0)
(1, 0)	(1, 0)	(0, 1)	(0, 0)	(1, 1)
(0, 1)	(0, 1)	(1, 0)	(1, 1)	(0, 0)

$\cdot$	(0, 0)	(1, 1)	(0, 1)	(1, 0)
(0, 0)	(0, 0)	(0, 0)	(0, 0)	(0, 0)
(1, 1)	(0, 0)	(1, 1)	(0, 1)	(1, 0)
(0, 1)	(0, 0)	(0, 1)	(0, 1)	(0, 0)
(1, 0)	(0, 0)	(1, 0)	(0, 0)	(1, 0)

We see from the tables $(1,1)$ is the only element that has a multiplicative inverse.

D. SUBRINGS. A nonempty subset S of a ring R is a **subring** of R if S is a ring with the same operations $+, \times$ restricted to S, and the same (additive and multiplicative) identities as R.

(1) If $S \subseteq R$ is nonempty and R is a ring, explain why it suffices to show that

- $0_R, 1_R \in S$,
- S is *closed under addition*: $s_1, s_2 \in S \Rightarrow s_1 + s_2 \in S$,
- S is *closed under additive inverses*: $s_1 \in S \Rightarrow -s_1 \in S$, and
- S is *closed under multipication*: $s_1, s_2 \in S \Rightarrow s_1 s_2 \in S$,

[3] We always mean "ring with identity" when we say "ring;" this differs from the book's convention

to show that S is a subring of R.

(2) Find subrings of each of $\mathbb{Q}$, $\mathbb{R}[x]$, and $\mathrm{Fun}(\mathbb{R},\mathbb{R})$.[4]

(3) Every ring always contains at least two "trivial" subrings. Explain.

(1) If S satisfies these conditions, then $+$ and $\times$ are operations on S (since S is closed under them). The fact that $+$ and $\times$ are associative, that $+$ is commutative, and the distributive property holds follows from the fact that these are true in R. The elements $0_R, 1_R \in S$ are identities for these two operations. Every element in S has an additive inverse because S is closed for additive inverses.

(2) $\mathbb{Z}$ is a subring of $\mathbb{Q}$, $\mathbb{Z}[x]$ is a subring of $\mathbb{R}[x]$, and the functions from $\mathbb{R}$ to $\mathbb{R}$ that are given by polynomials forms a subring of $\mathrm{Fun}(\mathbb{R},\mathbb{R})$.

(3) The ring R itself is always a subring of R. On the other hand, there is a smallest subring of R, which must include at least 0_R and 1_R. Then all the elements of the form

$$n\cdot 1_R = \underbrace{1_R+\cdots+1_R}_{n\text{ times}} \text{ and } -n\cdot 1_R = \underbrace{-1_R-\cdots-1_R}_{n\text{ times}}$$

should also be included; we can then prove that the set

$$\{n\cdot 1_R : n\in\mathbb{Z}\}$$

is always a subring of R.

E. ISOMORPHISM. Two rings R and S are **isomorphic** if they are "the same after relabling." More precisely, two rings are **isomorphic** if there is a **bijection** (called an **isomorphism**) between them that preserves addition and multiplication. We write $R \cong S$.

(1) Write out the + and $\times$ tables for $\mathbb{Z}_4$. There is a way to relabel the elements of $\mathbb{Z}_4$ with the names $a, b, c,$ and d, so that they each become one of operations ♣, ♢, ♡, and ♠ from below. Explain.

(2) Now use the card suits to put a ring structure on the set $S = \{a, b, c, d\}$. Find the additive and multiplicative identities. Explain why S is isomorphic to $\mathbb{Z}_4$.

(3) Prove or disprove: $\mathbb{Z}_2 \times \mathbb{Z}_2$ is isomorphic to $\mathbb{Z}_4$.

(4) Prove or disprove: *Isomorphism is an equivalence relation on the set of all rings.* This means that it is reflexive ($R \cong S$), symmetric ($R \cong S$ implies $S \cong R$) and transitive ($R \cong S$ and $S \cong T$ implies $S \cong T$).

♣	a	b	c	d
a	a	b	c	d
b	b	b	c	d
c	c	c	c	d
d	d	d	d	d

♢	a	b	c	d
a	a	d	c	b
b	b	a	d	c
c	c	b	a	d
d	d	c	b	a

♡	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	a	c
d	a	d	c	b

♠	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

[4] The set of all functions from $\mathbb{R}$ to itself with the "pointwise" operations $(f+g)(x) = f(x)+g(x)$ and $(fg)(x) = f(x)g(x)$.

(1)

·	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

We see that if we relabel $a \mapsto [0]$, $b \mapsto [1]$, $c \mapsto [2]$ and $[d] \mapsto [3]$, then these tables match up exactly with ♠ as addition and ♡ as multiplication.

(2) We can take the set S to be $\{a, b, c, d\}$, and the two binary operations ♠ to be the addition and ♡ to be the multiplication. By inspection, we see that both are commutative, and that a is the identity for ♠ (hence our “zero”) and b is the identity for ♡ (hence our ”1”). We see that every element has an additive identity (we can scan each row of the addition chart, looking for the zero element...we then can find what element is the additive inverse. So the additive inverse of a is a, the additive inverse of b is d (hence of d is b, and c is its own additive inverse). Checking the associative and distributive properties is a beast by hand, but it follow from the fact that these operations are just a relabeling of addition and multiplication in $\mathbb{Z}_4$, which we know are associative and distributive.

(3) Both $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ have four elements. However, there is no way to match up the elements so that $\mathbb{Z}_2 \times \mathbb{Z}_2 \cong \mathbb{Z}_4$. For example, if there were a way to match them up exactly, then the two rings would have to have the same number of elements that have multiplicative inverses. In $\mathbb{Z}_2 \times \mathbb{Z}_2$, there is only one (namely $(1, 1)$) but $\mathbb{Z}_4$ has two ($[1], [3]$).