Student: Yu Cheng (Jade)
Math 412
Worksheet #1
June 11, 2010

Worksheet #1

Problem A: Recall that a *ring* is an algebra $R = \langle R, +, -, \times, 0\rangle$ satisfying the axioms

1. $x + y = y + x$
2. $(x + y) + z = y + (x + z)$
3. $x + 0 = x$
4. $x + (-x) = 0$
5. $(xy)z = x(yz)$
6. $x(y + z) = xy + xz$ and $(y + z)x = yx + zx$

Some are commutative, some are not. Some have a multiplicative identity 1 or e, some do not. Give two examples of rings.

Answer $G = \langle \mathbb{Z}_3, +, \times\rangle$ forms a ring. With respect to the addition operation, G is associative and commutative, G has an identity element 0, and there is an addition inverse for every element in G. With respect to the multiplication operation, G is distributive, and the multiplication distributes over addition. Therefore, G is a ring. The characteristic tables of the addition and the multiplication operations on G are shown as below.

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$G = M_2(\mathbb{R})$ for all 2×2 matrices with the entries from $\mathbb{R}$ forms a ring. With respect to the addition operation, G is associative and commutative.

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \left(\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} + \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix}\right) = \begin{bmatrix} a_1 + a_2 + a_3 & b_1 + b_2 + b_3 \\ c_1 + c_2 + c_3 & d_1 + d_2 + d_3 \end{bmatrix}$$

$$= \left(\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}\right) + \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix}.$$

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{bmatrix} = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} + \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}.$$

With respect to the addition operation G has an identity element θ_2, and there is an additive inverse, $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$, for every element, $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G$.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

With respect to the multiplication operation, G is distributive.

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \cdot \left(\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \cdot \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix} \right)$$

$$= \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \cdot \begin{bmatrix} a_2a_3 + b_2c_3 & a_2b_3 + b_2d_3 \\ c_2a_3 + d_2c_3 & c_2b_3 + d_2d_3 \end{bmatrix}$$

$$= \begin{bmatrix} a_1(a_2a_3 + b_2c_3) + b_1(c_2a_3 + d_2c_3) & a_1(a_2b_3 + b_2d_3) + b_1(c_2b_3 + d_2d_3) \\ c_1(a_2a_3 + b_2c_3) + d_1(c_2a_3 + d_2c_3) & c_1(a_2b_3 + b_2d_3) + d_1(c_2b_3 + d_2d_3) \end{bmatrix}$$

$$= \begin{bmatrix} a_1a_2a_3 + a_1b_2c_3 + b_1c_2a_3 + b_1d_2c_3 & a_1a_2b_3 + a_1b_2d_3 + b_1c_2b_3 + b_1d_2d_3 \\ c_1a_2a_3 + c_1b_2c_3 + d_1c_2a_3 + d_1d_2c_3 & c_1a_2b_3 + c_1b_2d_3 + d_1c_2b_3 + d_1d_2d_3 \end{bmatrix}$$

$$\left(\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \cdot \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \right) \cdot \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix}$$

$$= \begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{bmatrix} \cdot \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix}$$

$$= \begin{bmatrix} (a_1a_2 + b_1c_2)a_3 + (a_1b_2 + b_1d_2)c_3 & (a_1a_2 + b_1c_2)b_3 + (a_1b_2 + b_1d_2)d_3 \\ (c_1a_2 + d_1c_2)a_3 + (c_1b_2 + d_1d_2)b_3 & (c_1a_2 + d_1c_2)b_3 + (c_1b_2 + d_1d_2)d_3 \end{bmatrix}$$

$$= \begin{bmatrix} a_1a_2a_3 + a_1b_2c_3 + b_1c_2a_3 + b_1d_2c_3 & a_1a_2b_3 + a_1b_2d_3 + b_1c_2b_3 + b_1d_2d_3 \\ c_1a_2a_3 + c_1b_2c_3 + d_1c_2a_3 + d_1d_2c_3 & c_1a_2b_3 + c_1b_2d_3 + d_1c_2b_3 + d_1d_2d_3 \end{bmatrix}.$$

The multiplication operation on G is distributes over the addition operation.

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \cdot \left(\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} + \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix} \right)$$

$$= \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \cdot \begin{bmatrix} a_2 + a_3 & b_2 + b_3 \\ c_2 + c_3 & d_2 + d_3 \end{bmatrix}$$

$$= \begin{bmatrix} a_1a_2 + b_1c_2 + a_1a_3 + b_1c_3 & a_1b_2 + b_1d_2 + a_1b_3 + b_1d_3 \\ c_1a_2 + d_1c_2 + c_1a_3 + d_1c_3 & c_1b_2 + d_1d_2 + c_1b_3 + d_1d_3 \end{bmatrix}$$

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \cdot \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} + \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \cdot \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix}$$

$$= \begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{bmatrix} + \begin{bmatrix} a_1a_3 + b_1c_3 & a_1b_3 + b_1d_3 \\ c_1a_3 + d_1c_3 & c_1b_3 + d_1d_3 \end{bmatrix}$$

$$= \begin{bmatrix} a_1a_2 + b_1c_2 + a_1a_3 + b_1c_3 & a_1b_2 + b_1d_2 + a_1b_3 + b_1d_3 \\ c_1a_2 + d_1c_2 + c_1a_3 + d_1c_3 & c_1b_2 + d_1d_2 + c_1b_3 + d_1d_3 \end{bmatrix}.$$

Problem B: Prove the following statements about rings.

a. If $x + y = x + z$, then $y = z$.

Answer According to the axiom that there is an addictive inverse for every element in a ring, there exist an element $-x$, such that $(-x) + x = 0$

$$x + y = x + z$$

$$\Rightarrow (-x) + x + y = (-x) + x + z$$

$$\Rightarrow y = z\,.$$

b. The additive identity of R is unique.

Answer Assume we have two different additive identities for R, and they are e_1 and e_2.

$$x + e_1 = x = x + e_2$$

$$\Rightarrow x + e_1 = x + e_2\,.$$

According to the previous statement, $x + y = x + z$ derives $y = z$, we have,

$$x + e_1 = x + e_2$$

$$\Rightarrow e_1 = e_2\,.$$

Therefore, we can't have two different additive identities, the additive identity of R is unique.

c. The additive inverse of an element x is unique.

Answer Assume we have two different additive inverses of element x, and they are $(-x)_1$ and $(-x)_2$.

$$x + (-x)_1 = e = x + (-x)_2$$

$$\Rightarrow x + (-x)_1 = x + (-x)_2\,.$$

According to the first statement, $x + y = x + z$ derives $y = z$, we have,

$$x + (-x)_1 = x + (-x)_2$$

$$\Rightarrow (-x)_1 = (-x)_2\,.$$

Therefore, we can't have two different inverses for element x, the additive inverse of x is unique.

d. If $xy = xz$ and $x \neq 0$, what can we conclude?

Answer For regular ring, we can't conclude $y = z$. But if the ring R is also a *integral domain*, that is a commutative ring with identity and for every $a, b \in R$ such that $ab = 0$, either $a = 0$ or $b = 0$, then we can conclude $y = z$.

$$xy = xz$$

$$\Rightarrow xy - xz = xz - xz = 0$$

$$\Rightarrow xy - xz = 0$$

$$\Rightarrow x(y - z) = 0$$

$$\Rightarrow x = 0 \;\; or \;\; y - z = 0$$

$$\Rightarrow y - z = 0$$

$$\Rightarrow y - z + z = 0 + z$$

$$\Rightarrow y = z\,.$$

e. What if $xy = xz$ and x has a multiplicative inverse? (In this case, R must have an identity element 1)

Answer We can conclude $y = z$. In this case when we have a multiplicative identity.

$$xy = xz \Rightarrow \frac{1}{x} \cdot (x \cdot y) = \frac{1}{x} \cdot (x \cdot z)$$

$$\Rightarrow \left(\frac{1}{x} \cdot x\right) \cdot y = \left(\frac{1}{x} \cdot x\right) \cdot z \Rightarrow 1 \cdot y = 1 \cdot x$$

$$\Rightarrow y = z\,.$$

f. $x0 = 0x = 0$

Answer We will start from the left side.

$$x \cdot 0 = x \cdot (0 + 0) = (x \cdot 0) + (x \cdot 0)$$

$$\Rightarrow x \cdot 0 = (x \cdot 0) + (x \cdot 0)$$

$$\Rightarrow (x \cdot 0) + \big(-(x \cdot 0)\big) = (x \cdot 0) + (x \cdot 0) + \big(-(x \cdot 0)\big)$$

$$\Rightarrow 0 = x \cdot 0\,.$$

g. $x(-y) = -xy$

Answer We will derive the given statement from $x0 = 0$.

$$x \cdot 0 = 0$$

$$\Rightarrow x \cdot \big(y + (-y)\big) = 0$$

$$\Rightarrow (x \cdot y) + \big(x \cdot (-y)\big) = 0$$

$$\Rightarrow x \cdot y + x \cdot (-y)$$

$$\Rightarrow x \cdot (-y) = -x \cdot y\,.$$

h. $-x(y) = -xy$

Answer We will derive the given statement from $0y = 0$.

$$0 \cdot y = 0$$

$$\Rightarrow \big((-x) + x\big) \cdot y = 0$$

$$\Rightarrow (-x) \cdot y + x \cdot y = 0$$

$$\Rightarrow (-x) \cdot y = -x \cdot y$$

$$\Rightarrow -x \cdot (y) = -x \cdot y\,.$$

Problem C: Let R be a ring and $a \in R$. Prove that $\{x \in R : ax = 0\}$ is a sub-ring of R.

Answer Let $G = \{x \in R : ax = 0\}$ and $x_1 \in G, x_2 \in G$. G is closed by addition.

$$ax_1 + ax_2 = 0 + 0 = 0$$

$$\Rightarrow a \cdot (x_1 + x_2) = 0$$

$$\Rightarrow x_1 + x_2 \in G\,.$$

G is also closed by multiplication.

$$ax_1 = 0$$

$$\Rightarrow (ax_1) \cdot x_2 = 0 \cdot x_2 = 0 \;\text{ since } x \in R$$

$$\Rightarrow a \cdot (x_1 x_2) = 0$$

$$\Rightarrow x_1 x_2 \in G\,.$$

Axiom 1, 2, 5, 6 hold because $x \in R$ for all $x \in G$. G also has an additive identity, which is the same, 0, as R's

$$x + 0 = x$$

$$\Rightarrow a \cdot (x + 0) + a \cdot x$$

$$\Rightarrow (a \cdot x) + (a \cdot 0) \;= a \cdot x$$

$$\Rightarrow a \cdot 0 = 0$$

$$\Rightarrow 0 \in G\,.$$

Every element in G has an additive inverse, which is the same as in R.

$$x + (-x) = 0$$

$$\Rightarrow a \cdot \big(x + (-x)\big) = a \cdot 0$$

$$\Rightarrow (a \cdot x) + \big(a \cdot (-x)\big) \;= 0 = a \cdot x$$

$$\Rightarrow a \cdot (-x) = 0$$

$$\Rightarrow -x \in G\,.$$

Problem D: Consider the integers with the operations

$$a \oplus b = a + b - 1$$

$$a \odot b = a + b - ab$$

Show hat this defines a commutative ring with unit.

Answer Since $(a + b - 1)$ and $(a + b - ab)$, where $a, b \in \mathbb{Z}$, are always integers, the given groupoid G is closed under addition and multiplication. G is commutative with respect to the addition operation.

$$a \oplus b = a + b - 1 = \; b \oplus a\,.$$

G is distributive with respect to the addition operation.

$$a \oplus (b \oplus c) = a \oplus (b + c - 1)$$

$$= a + (b + c - 1) - 1$$

$$= a + b + c - 2$$

$$(a \oplus b) \oplus c = (a + b - 1) \oplus c$$

$$= (a + b - 1) + c - 1$$

$$= a + b + c - 2$$

$$\Rightarrow a \oplus (b \oplus c) = (a \oplus b) \oplus c\,.$$

There is an additive identity, 1, in G.

$$a \oplus 1 = 1 \oplus a = a + 1 - 1 = a\,.$$

There is a additive inverse, $(2 - a)$, for all $a \in G$.

$$a \oplus (2 - a) = a + (2 - a) - 1 = 1\,.$$

G is distributive with respect to the multiplication operation.

$$\begin{aligned}
a \odot (b \odot c) &= a \odot (b + c - bc) \\
&= a + (b + c - bc) - a(b + c - bc) \\
&= abc - ab - ac - bc + a + b + c \\
(a \odot b) \odot c &= (a + b - ab) \odot c \\
&= (a + b - ab) + c - (a + b - ab)c \\
&= abc - ab - ac - ab + a + b + c \\
\Rightarrow a \odot (b \odot c) &= (a \odot b) \odot c\,.
\end{aligned}$$

The multiplication operation distribute over addition.

$$\begin{aligned}
a \odot (b \oplus c) &= a \odot (b + c - 1) \\
&= a + (b + c - 1) - a(b + c - 1) \\
&= -ab - ac + b + c - 1 \\
(a \odot b) \oplus (a \odot c) &= (a + b - ab) \oplus (a + c - ac) \\
&= a + b - ab + a + c - ac - 1 \\
&= -ab - ac + b + c - 1 \\
\Rightarrow a \odot (b \oplus c) &= (a \odot b) \oplus (a \odot c)\,.
\end{aligned}$$

The multiplication operation is commutative.

$$a \odot b = b \odot a = a + b - ab\,.$$

There is a multiplicative identity, 0.

$$a \odot 0 = 0 \odot a = a + 0 - a0 = a\,.$$

In summary, integer group with operations $a \oplus b = a + b - 1$ and $a \odot b = a + b - ab$ is a commutative ring with unit, 0.

Problem E: Can every ring be embedded into a ring with a multiplicative identity? How?

Answer Yes, any ring, R can be embedded into a ring with a multiplicative identity. We define a set of ordered pairs. $G = \{(n, r) | n \in \mathbb{Z}, r \in R\}$ with the following operations.

$$(n, r) + (m, s) = (n + m, r + s)$$

$$(n, r) \cdot (m, s) = (nm, ns + mr + rs)$$

We will also define the following elementary operation for nr, where $n \in \mathbb{Z}$, $r \in R$.

$$nr = \begin{cases} 0 & \text{if } n = 0 \\ \underbrace{r + r + \cdots + r}_{n \text{ times}} & \text{if } n > 0 \\ -((-n)r) & \text{if } n < 0 \end{cases}$$

We can show that G is a ring with multiplicative identity. Obviously G is closed under addition, since $\mathbb{Z}, R$ are rings and $n + m \in \mathbb{Z}$ and $r + s \in R$.

$$r + s \in R \text{ since } r \in R, s \in R, R \text{ is a ring}$$

$$n + m \in \mathbb{Z} \text{ since } n \in \mathbb{Z}, m \in v, \mathbb{Z} \text{ is a ring}$$

$$\Rightarrow (n + m, r + s) \in G\ .$$

G is also closed under multiplication. According to the definition, $nr \in R$

$$ns \in R, mr \in R$$

$$rs \in R \text{ since } r \in R, s \in R, R \text{ is a ring}$$

$$\Rightarrow ns + mr + rs \in R$$

$$nm \in \mathbb{Z} \text{ since } n \in \mathbb{Z}, m \in v, \mathbb{Z} \text{ is a ring}$$

$$\Rightarrow (nm, ns + mr + rs) \in G\ .$$

G is commutative under the addition operation.

$$(n, r) + (m, s) = (n + m, r + s)$$

$$(m, s) + (n, r) = (m + n, s + r)$$

$$\Rightarrow n + m = m + n \text{ since } \mathbb{Z} \text{ is a ring}$$

$$\Rightarrow r + s = s + r \text{ since } R \text{ is a ring}$$

$$\Rightarrow (n, r) + (m, s) = (m, s) + (n, r)\ .$$

G is associative under the addition operation.

$$\begin{aligned}(n,r)+\big((m,s)+(o,t)\big)&=(n,r)+(m+o,s+t)\\&=(n+m+o,r+s+t)\\\big((n,r)+(m,s)\big)+(o,t)&=(n+m,r+s)+(o,t)\\&=(n+m+o,r+s+t)\end{aligned}$$

$$\Rightarrow (n,r)+\big((m,s)+(o,t)\big)=\big((n,r)+(m,s)\big)+(o,t)\,.$$

G has a additive identity $(0,0)$.

$$(n,r)+(0,0)=(0,0)+(n,r)=(n,r)\ \text{ since }\ \mathbb{Z}\,R\text{ are rings}\,.$$

Every element, (n,r), in G has an additive inverse, $(-n,-r)$

$$(n,r)+(-n,-r)=(0,0)\ \text{ since }\ \mathbb{Z}\,R\text{ are rings}\,.$$

G is associative under the multiplication operation. Note $nr_1+nr_2=n(r_1+r_2)$, $n_1n_2r=n_2n_1r$, $r_1nr_2=nr_1r_2$ where $n,n_1,n_2\in\mathbb{Z}$, $r,r_1,r_2\in R$.

$$\begin{aligned}(n,r)\cdot\big((m,s)\cdot(o,t)\big)&=(n,r)\cdot(mo,mt+os+st)\\&=\big(nmo,n(mt+os+st)+mor+r(mt+os+st)\big)\\&=(nmo,nmt+nos+nst+mor+rmt+ros+rst)\\\big((n,r)\cdot(m,s)\big)\cdot(o,t)&=(nm,ns+mr+rs)\cdot(o,t)\\&=(nmo,nmt+o(ns+mr+rs)+(ns+mr+rs)t)\\&=(nmo,nmt+ons+omr+ors+nst+mrt+rst)\end{aligned}$$

$$\Rightarrow (n,r)\cdot\big((m,s)\cdot(o,t)\big)=\big((n,r)\cdot(m,s)\big)\cdot(o,t)\,.$$

The multiplication operation is distributive over addition.

$$\begin{aligned}(n,r)\cdot\big((m,s)+(o,t)\big)&=(n,r)\cdot(m+o,s+t)\\&=\big(n(m+o),n(s+t)+(m+o)r+r(s+t)\big)\\&=(nm+no,ns+nt+mr+or+rs+rt)\\(n,r)\cdot(m,s)+(n,r)\cdot(o,t)&=(nm,ns+mr+rs)+(no,nt+or+rt)\\&=(nm+no,ns+mr+rs+nt+or+rt)\end{aligned}$$

$$\Rightarrow (n,r)\cdot\big((m,s)+(o,t)\big)=(n,r)\cdot(m,s)+(n,r)\cdot(o,t)\,.$$

G has a multiplicative identity, $(1, 0)$.

$$\begin{aligned}(n, r) \cdot (1, 0) &= (n1, n0 + 1r + r0) \\ &= (n, r) \\ (1, 0) \cdot (n, r) &= (1n, 1r + n0 + 0r) \\ &= (n, r) \\ \Rightarrow (n, r) \cdot (1, 0) &= (1, 0) \cdot (n, r) = (n, r)\,.\end{aligned}$$

In summary, we've shown that any ring R can be embedded into a ring with multiplicative identity. Namely, the newly created ring is (n, r), where $n \in \mathbb{Z}$ and $r \in R$.