Assignment Five

Lizzy Hunt

February 17, 2023

1 Section 3.2

1.1 Question One

1.1.1 a

$a^2 - ab + ba - b^2$

1.1.2 b

$a^3 + ba^2 + 2a^2b + 2ab^2 + ab^2 + b^3$

1.1.3 c

(a) could be $a^2 - b^2$
(b) could be $a^3 + 3a^2b + 3ab^2 + b^3$

1.2 Question Three

1.2.1 a

$\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}, \begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}, \begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}, \begin{smallmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}$

1.2.2 b

```
>>> set(filter(lambda y: all([y**2 % 12 == y for x in range(12)]), range(12)))
{0, 1, 4, 9}
```

1.3 Question Seven

S is closed under multiplication: $i \in S, j \in S \Rightarrow i \cdot j = n1_R \cdot m1_R = (nm)1_R$.
S is closed under subtraction: $i \in S, j \in S \Rightarrow i - j = n1_R - m1_R = (n-m)1_R$

1.4 Question Eight

Considering $n, m \in T$ then $n = xb, m = yb$ with $x, y \in R$:

1. T is closed under multiplication: $n \cdot m = xb \cdot yb = (x \cdot y)b$, which follows the rule.
2. T is closed under subtraction: $n - m = xb - yb = (x - y)b$, which also follows the rule.

We also know T is not empty since it must have at least 0_{R}.

1.5 Question Ten

1.5.1 a

$\bar{R} = (0,0), (1,0), (2,0)$
$\bar{S} = (0,0), (0,1), (0,2), (0,3), (0,4)$

1.5.2 b

Considering $n, m \in \bar{R}$, then $n = (x, 0_S), n = (y, 0_S)$ with $x, y \in R$.

1. $\bar{R}$ is closed under multiplication: $n \cdot m = (x, 0_S) \cdot (y, 0_S) = (x \cdot y, 0_S)$ and $x \cdot y \in R$, so thus $n \cdot m \in R \times S$.
2. $\bar{R}$ is closed under subtraction: $n - m = (x, 0_S) - (y, 0_S) = (x - y, 0_S)$ and $x - y \in R$, so thus $n - m \in R \times S$.

We also know that $\bar{R}_0 = (0_R, 0_S) \in R \times S$ so $\bar{R}$ is not empty.

1.5.3 c

Considering $n, m \in \bar{S}$, then $n = (0_R, x), n = (0_R, y)$ with $x, y \in S$.

1. $\bar{S}$ is closed under multiplication: $n \cdot m = (0_R, x) \cdot (0_R, y) = (x \cdot y, 0_S)$ and $x \cdot y \in S$, so thus $n \cdot m \in R \times S$.
2. $\bar{S}$ is closed under subtraction: $n - m = (0_R, x) - (0_R, y) = (0_R, x - y)$ and $x - y \in R$, so thus $n - m \in R \times S$.

We also know that $\bar{S}_0 = (0_R, 0_S) \in R \times S$ so $\bar{S}$ is not empty.

1.6 Question Thirteen

1.6.1 a

Considering $n, m \in S \cap T$, then $n \in S$ and $n \in T$, $m \in S$ and $m \in T$, therefore:

1. $S \cap T$ is closed under multiplication as $m \cdot n$ must also be in $S \cap T$
2. $S \cap T$ is closed under addition as $m + n$ must also be in $S \cap T$

Since S and T are both subrings of R, $0_R \in S \cap T$.

1.6.2 b

No, consider S being the integer multiples of 8 and T being the integer multiples of 3 being subrings of $\mathbb{Z}$ (proof of these being subrings is in Question Six of Section 3.1 in Assignment Four), then $n \in S$ with $n = 8$ and $m \in T$ with $m = 3$ then $n + m = 11 \notin S \cup T$.

1.7 Question Fifteen - TODO

1.8 Question Twenty-One

1.8.1 a

From $ab = ac \Rightarrow ab - ac = 0_R \Rightarrow a(b - c) = 0_R$, we know $b - c$ is equivalent to 0_R since we're given that a is a non-zero element.
$b - c = 0_R \Rightarrow b = c$

1.8.2 b

From $ba = ca \Rightarrow ba - ca = 0_R \Rightarrow (b - c)(a) = 0_R$ we come to the same conclusion as (a)
$b - c = 0_R \Rightarrow b = c$

2 Section 3.3

2.1 Question One

In the true nature of being a computer science student, automate something for 2 hours that you could've done in 20 minutes!

```
cartesian_prod = lambda zn, zm: list([(i, j) for i in range(zn) for j in range(zm)])
mult_tup = lambda a, b, zn, zm: ((a[0] * b[0]) % zn, (a[1] * b[1]) % zm)
add_tup = lambda a, b, zn, zm: ((a[0] + b[0]) % zn, (a[1] + b[1]) % zm)
empty_table = lambda col, row, symbol: [[symbol] + [str(x) for x in col]] + [[str(x)] + [0 for i in range(len(col))] for x in row]

def make_cartesian_congruence_table(zn, zm, op, mapping, symbol):
  cp = cartesian_prod(zn, zm)
  mapped_cp = [cp[mapping[i]] for i in range(len(cp))]
  table = empty_table(mapped_cp, mapped_cp, symbol)
  for i in range(len(cp)):
    for j in range(len(cp)):
      table[i+1][j+1] = str(op(mapped_cp[i], mapped_cp[j], zn, zm))
  return table

def make_normal_table(n, op, symbol):
  table = empty_table(list(range(n)), list(range(n)), symbol)
  for i in range(n):
    for j in range(n):
      table[i+1][j+1] = str(op(i, j) % n)
  return table
```

2.1.1 $\mathbf{Z_2} \times \mathbf{Z_3}$ with bijection

```
bijection = [0, 4, 2, 3, 1, 5]
```

1. Multiplication Tables

```
make_cartesian_congruence_table(2, 3, mult_tup, bijection, '\odot')
```

$\odot$	(0, 0)	(1, 1)	(0, 2)	(1, 0)	(0, 1)	(1, 2)
(0, 0)	(0, 0)	(0, 0)	(0, 0)	(0, 0)	(0, 0)	(0, 0)
(1, 1)	(0, 0)	(1, 1)	(0, 2)	(1, 0)	(0, 1)	(1, 2)
(0, 2)	(0, 0)	(0, 2)	(0, 1)	(0, 0)	(0, 2)	(0, 1)
(1, 0)	(0, 0)	(1, 0)	(0, 0)	(1, 0)	(0, 0)	(1, 0)
(0, 1)	(0, 0)	(0, 1)	(0, 2)	(0, 0)	(0, 1)	(0, 2)
(1, 2)	(0, 0)	(1, 2)	(0, 1)	(1, 0)	(0, 2)	(1, 1)

2. Addition Tables

```
make_cartesian_congruence_table(2, 3, add_tup, bijection, '\oplus')
```

$\oplus$	(0, 0)	(1, 1)	(0, 2)	(1, 0)	(0, 1)	(1, 2)
(0, 0)	(0, 0)	(1, 1)	(0, 2)	(1, 0)	(0, 1)	(1, 2)
(1, 1)	(1, 1)	(0, 2)	(1, 0)	(0, 1)	(1, 2)	(0, 0)
(0, 2)	(0, 2)	(1, 0)	(0, 1)	(1, 2)	(0, 0)	(1, 1)
(1, 0)	(1, 0)	(0, 1)	(1, 2)	(0, 0)	(1, 1)	(0, 2)
(0, 1)	(0, 1)	(1, 2)	(0, 0)	(1, 1)	(0, 2)	(1, 0)
(1, 2)	(1, 2)	(0, 0)	(1, 1)	(0, 2)	(1, 0)	(0, 1)

2.1.2 $\mathbf{Z_6}$

1. Multiplication Tables

```
make_normal_table(6, lambda a, b: a * b, '\odot')
```

$\odot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

2. Addition Tables

```
make_normal_table(6, lambda a, b: a + b, '\oplus')
```

$\oplus$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

2.2 Question Two

```
bijection = [0, 3, 2, 1]
make_cartesian_congruence_table(2, 2, mult_tup, bijection, '\odot')
```

$\odot$	(0, 0)	(1, 1)	(1, 0)	(0, 1)
(0, 0)	(0, 0)	(0, 0)	(0, 0)	(0, 0)
(1, 1)	(0, 0)	(1, 1)	(1, 0)	(0, 1)
(1, 0)	(0, 0)	(1, 0)	(1, 0)	(0, 0)
(0, 1)	(0, 0)	(0, 1)	(0, 0)	(0, 1)

```
bijection = [0, 3, 2, 1]
make_cartesian_congruence_table(2, 2, add_tup, bijection, '\oplus')
```

$\oplus$	(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)

2.3 Question Three

1. f is injective, since $f(a) = f(b) \Rightarrow (a, a) = (b, b) \Rightarrow a = b$
2. f is surjective since every range element in R^*, (a, a) is mapped to $a \in R$ by definition
3. $f(a) + f(b) = (a, a) + (b, b) = (a + b, a + b) = f(a + b)$ and $f(a)f(b) = (a, a) \cdot (b, b) = (ab, ab) = f(ab)$

2.4 Question Four

$f(1)f(3) = (2)(6) \equiv_{10} 2$ but $f(3) = 6$ which doesn't hold the properties of homomorphism.

2.5 Question Five

Consider the given function:

1. f is injective, since $f(a) = f(b) \Rightarrow \begin{smallmatrix} 0 & 0 \\ 0 & a \end{smallmatrix} = \begin{smallmatrix} 0 & 0 \\ 0 & b \end{smallmatrix} \Rightarrow a = b$
2. f is surjective, since every range element $\begin{smallmatrix} 0 & 0 \\ 0 & a \end{smallmatrix}$ has an element in $\mathbb{R}$, a, such that $f(a) = \begin{smallmatrix} 0 & 0 \\ 0 & a \end{smallmatrix}$ by definition
3. $f(a) + f(b) = \begin{smallmatrix} 0 & 0 \\ 0 & a \end{smallmatrix} + \begin{smallmatrix} 0 & 0 \\ 0 & b \end{smallmatrix} = \begin{smallmatrix} 0 & 0 \\ 0 & (a+b) \end{smallmatrix} = f(a + b)$, and $f(a) \cdot f(b) = \begin{smallmatrix} 0 & 0 \\ 0 & a \end{smallmatrix} \cdot \begin{smallmatrix} 0 & 0 \\ 0 & b \end{smallmatrix} = \begin{smallmatrix} 0 & 0 \\ 0 & (a \cdot b) \end{smallmatrix} = f(a \cdot b)$,

2.6 Question Nine - TODO

2.7 Question Eleven

2.7.1 b

```
>>> f = lambda x: 3 * x
>>> list(filter(lambda x: f(x * x) != (f(x) * f(x)), range(0, 20, 2)))
[2, 4, 6, 8, 10, 12, 14, 16, 18]
```

2.7.2 d

```
>>> k = lambda x: 0 if x == 0 else (x ** -1)
>>> list(filter(lambda x: k(x * x) != (k(x) * k(x)), range(0, 20)))
[5, 10, 13, 19]
```

2.8 Question Twelve

2.8.1 c

Not a homomorphism. Just from reducing $f(x+x)$ we find $f(x+x) \neq f(x)+f(x)$:

$$f(x+x) = \frac{1}{(x+x)^2+1} = \frac{1}{4x^2+1}$$

$$f(x)+f(x) = \frac{1}{x^2+1} + \frac{1}{x^2+1} = \frac{2}{x^2+1}$$

Thus $f(x+x) \neq f(x)+f(x)$.

2.8.2 d

```
>>> import numpy as np
>>> h = lambda x: [[-x, 0], [x, 0]]
>>> list(filter(lambda x: not np.array_equiv(h(x * x), np.dot(h(x), h(x))), range(0, 20))
[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19]
```

2.9 Question Thirteen

2.9.1 a

If $r \in R$ then $(r, 0_S) \in R \times S$, and $f((r, 0_S)) = r$, so every range element has a domain element mapping to it.
For some $a = (r, m) \in R \times S$ and $b = (t, v) \in R \times S$ then $f((r, m)) + f((t, v)) = r + t = f((r+t, v+m))$, and $f((r, m)) \cdot f((t, v)) = r \cdot t = f((r \cdot t, v \cdot m))$.

2.9.2 b

If $s \in S$ then $(0_R, s) \in R \times S$, and $f((0_R, s)) = s$, so every range element has a domain element mapping to it.
For some $a = (r, m) \in R \times S$ and $b = (t, v) \in R \times S$ then $f((r, m)) + f((t, v)) = m + v = f((r+t, m+v))$, and $f((r, m)) \cdot f((t, v)) = m \cdot v = f((r \cdot t, m \cdot v))$.

2.10 Question Fifteen

Consider $f : Z_4 \to Z_4 \ni f(x) = 0$, then 2 is a zero divisor, but 0 is not by definition.

2.11 Question Twenty One

2.11.1 Lemma

We assume a multiplicative identity x exists in $\mathbb{Z}^*$:
$b \odot x = b \Rightarrow b + x - bx = b \Rightarrow x - bx = 0 \Rightarrow x(1-b) = 0$ and $1 - b \neq 0 \forall b \in \mathbb{Z}^*$ so $x = 0$.
which is verified by:
$0 \odot b = 0 + b - 0 \cdot b = b$ and $b \odot 0 = b + 0 - b \cdot 0 = b$.

2.11.2 Proof

Consider $f : \mathbb{Z} \to \mathbb{Z}^*$ to be the isomorphism we so desire, then by Theorem 3.10, f(1 ∈ Z) = 0 ∈ Z*.
Therefore, f(2) = f(1 + 1) = f(1) ⊕ f(1) = -1, f(3) = f(2 + 1) = -1 ⊕ f(1) = -2.
$f : \mathbb{Z} \to \mathbb{Z}^* \ni f(x) = 1 - x$ seems to fit the bill nicely.

1. f is a bijection since we have an inverse $x = 1 - f(x)$
2. $f(a \oplus b) = 1 - (a \oplus b) = 1 - (a + b - 1) = (1 - a) + (1 - b) = f(a) + f(b)$ and $f(a \odot b) = 1 - (a \odot b) = 1 - (a + b - ab) = (1 - a) \cdot (1 - b) = f(a) \cdot f(b)$

2.12 Question Twenty Four

2.12.1 a

1. By the usual coordinate addition we know that $a, b \in R \Rightarrow a + b \in R$ and is associative, commutative, and the additive identity is $(0, 0)$.
2. R is closed under multiplication: $a, b \in R \Rightarrow a = (c, d) \wedge b = (e, f) \Rightarrow a \cdot b = (ce, de)$ and since $c, d, e, f \in \mathbb{R}$ then $(ce, de) \in \mathbb{R} \times \mathbb{R}$ by definition.
3. Multiplication is associative: $a, b, c \in R \Rightarrow a = (d, e) \wedge b = (f, g) \wedge c = (h, i) \Rightarrow (a \cdot b) \cdot c = (df, ef) \cdot (h, i) = (dfh, efh)$ and $a \cdot (b \cdot c) = (d, e) \cdot (fh, gh) = (dfh, efh)$
4. Multiplication is distributive: $a, b, c \in R \Rightarrow a = (d, e) \wedge b = (f, g) \wedge c = (h, i) \Rightarrow a(b + c) = (e, f) \cdot (f + h, g + i) = (ef + eh, ff + fh) = (ef, ff) + (eh, fh) = a \cdot b + a \cdot c$ and $a, b, c \in R \Rightarrow a = (d, e) \wedge b = (f, g) \wedge c = (h, i) \Rightarrow (a + b) \cdot c = (d + f, e + g) \cdot (h, i) = (dh + fh, eh + gh) = (dh, eh) + (fh, gh) = a \cdot c + b \cdot c$

2.12.2 b

Consider the function $f : R \to M(\mathbb{R})$ is an isomorphism, such that $f((a,b)) = \begin{smallmatrix} a & 0 \\ b & 0 \end{smallmatrix}$, then:

1. f is surjective since every element in the range has a domain element $\begin{smallmatrix} a & 0 \\ b & 0 \end{smallmatrix} = y \ni f((a,b)) = y$
2. f is injective since $f((c,d) = x) = f((e,f) = y) \Rightarrow \begin{smallmatrix} c & 0 \\ d & 0 \end{smallmatrix} = \begin{smallmatrix} e & 0 \\ f & 0 \end{smallmatrix} \Rightarrow c = e \wedge d = f \Rightarrow x = y$
3. $f((c,d) = x) + f((e,f) = y) \Rightarrow \begin{smallmatrix} c & 0 \\ d & 0 \end{smallmatrix} + \begin{smallmatrix} e & 0 \\ f & 0 \end{smallmatrix} = \begin{smallmatrix} c+e & 0 \\ d+f & 0 \end{smallmatrix} = f(x+y)$, and $f((c,d) = x) \cdot f((e,f) = y) \Rightarrow \begin{smallmatrix} c & 0 \\ d & 0 \end{smallmatrix} \cdot \begin{smallmatrix} e & 0 \\ f & 0 \end{smallmatrix} = \begin{smallmatrix} ce & 0 \\ de & 0 \end{smallmatrix} = f(x \cdot y)$