MTH 343 Homework 1

Philip Warton

April 10, 2020

1.3

(1) 1.3.13

Proof. $\boxed{A \setminus (B \cup C) \subset (A \setminus B) \cap (A \setminus C)}$

Let $x \in A \setminus (B \cup C)$. We know that $x \in A$ and $x \notin B \cup C$, thus $x \notin B$ and $x \notin C$. Since $x \in A$ and $x \notin B$, $x \in A \setminus B$. Similarly since $x \notin C, x \in A \setminus C$, thus $x \in (A \setminus B) \cap (A \setminus C)$, and thus $A \setminus (B \cup C) \subset (A \setminus B) \cap (A \setminus C)$.

$\boxed{A \setminus (B \cup C) \supset (A \setminus B) \cap (A \setminus C)}$

Let $x \in (A \setminus B) \cap (A \setminus C)$. Then $x \in A$ and $x \notin B$ and $x \notin C$. Thus $x \notin B \cup C$, and it follows that $x \in A \setminus (B \cup C)$. Therefore $A \setminus (B \cup C) \supset (A \setminus B) \cap (A \setminus C)$. And we say that the two sets are equal. □

(2) 1.3.18

(a)

Let f be a function $f : \mathbb{R} \to \mathbb{R}$ where $f(x) = e^x$.

$\boxed{1:1}$ Let $x, y \in \mathbb{R}$ such that $f(x) = f(y)$. Then $e^x = e^y$, and we can take the natural log of both sides which gives $x = y$. Thus f is one-to-one.

$\boxed{\text{Onto}}$ For f to be onto, for all $y \in \mathbb{R}$ there must exist some $x \in \mathbb{R}$ such that $f(x) = y$. Let $y = -1$, then there should be some x such that $f(x) = e^x = -1$. Since this equation has no solutions, f is not onto. If $y > 0$ then $\exists x : f(x) = y$, so we say that the range of f is $(0, \infty)$.

(b)

Let f be a function $f : \mathbb{Z} \to \mathbb{Z}$ where $f(n) = n^2 + 3$.

$\boxed{1:1}$ Let $m, n \in \mathbb{N}$ such that $f(m) = f(n)$. Then we say that $m^2 + 3 = n^2 + 3$, which is equivalent to saying that $m^2 = n^2$. This does not guarentee that $m = n$, because the case where $m = -n$ is a also a solution, therefore f is not one-to-one.

$\boxed{\text{Onto}}$ Let $f(n) = 0 \in \mathbb{Z}$, then

$$\begin{aligned} n^2 + 3 &= 0 \\ n^2 &= -3 \\ n &= \sqrt{-3} \end{aligned}$$

Since this has no solutions, f is not onto. The range of f is $[3, \infty) \cap \mathbb{Z}$.

(c)

Let f be a function $f : \mathbb{R} \to \mathbb{R}$ where $f(x) = \sin(x)$.

$\boxed{1:1}$ Let $x = 0$ and $y = 2\pi$, then $f(x) = f(y) = 0$, but $x \neq y$. Therefore f is not one-to-one.

$\boxed{\text{Onto}}$ Since $-1 \leqslant \sin(x) \leqslant 1$, f is not onto and its range is $[-1, 1]$.

(d)

Let f be a function $f : \mathbb{Z} \to \mathbb{Z}$ where $f(n) = n^2$.

$\boxed{1:1}$ Choose $m = 1, n = -1$, then $f(m) = f(n)$ but $m \neq n$, so f is not one-to-one.

$\boxed{\text{Onto}}$ We know that $n^2 \geqslant 0$ for all $n \in \mathbb{Z}$, so f is not onto and its range is $\{n \in \mathbb{Z} \mid \sqrt{n} \in \mathbb{Z}\}$

(3) 1.3.22

Let $f : A \to B$ and $g : B \to C$.

(a)

Suppose f and g are one-to-one. Show $g \circ f$ is one-to-one.

Proof. Let $a_1, a_2 \in A$ such that $g \circ f(a_1) = g \circ f(a_2)$. Since g is one-to-one, we know that $f(a_1) = f(a_2)$. Since f is one-to-one, it follows that $a_1 = a_2$, therefore $g \circ f$ is one-to-one as well $\square$

(b)

Show that $g \circ f$ is onto $\Longrightarrow$ g is onto.

Proof. Suppose that $g \circ f$ is onto. Then for all $c \in C$ there exists some $a \in A$ such that $g \circ f(a) = c$. Let $c \in C$ be arbitrary. Then, there $\exists a \in A$ such that $c = g(f(a))$. We know that $f : A \to B$, so $f(a) \in B$. Thus, there exists $b = f(a) \in B$ such that $g(b) = c$, therefore g is onto. $\square$

(c)

Show that $g \circ f$ is one-to-one $\Longrightarrow$ f is one-to-one.

Proof. Assume that $g \circ f$ is one-to-one. If $g(f(a_1)) = g(f(a_2))$ then $a_1 = a_2$ for any $a_1, a_2 \in A$. We want to show that $x \neq y \Longrightarrow f(x) \neq f(y)$. Let $x, y \in A$ such that $x \neq y$. Then, by assumption, $g(f(x)) \neq g(f(y))$. Suppose by contradiction that $f(x) = f(y)$, then since g is a function it follows that $g(f(x)) = g(f(y))$ (contradiction). Therefore $f(x)$ must not equal $f(y)$, and we say that f is one-to-one. $\square$

(d)

Show that $g \circ f$ is one-to-one and f is onto $\Longrightarrow$ g is one-to-one.

Proof. Assume that $g \circ f$ is one-to-one and that f is onto. We want to show that $g(b_1) = g(b_2) \Longrightarrow b_1 = b_2 \;\; \forall b_1, b_2 \in B$. Let $b_1, b_2 \in B$ such that $g(b_1) = g(b_2)$ without loss of generality. Then since f is onto, we know that $\exists a_1, a_2 \in A$ such that $f(a_1) = b_1$ and $f(a_2) = b_2$. Therefore, $g(f(a_1)) = g(f(a_2))$, and since $g \circ f$ is one-to-one, it follows that $a_1 = a_2$. Since g is well-defined and $a_1 = a_2$, $b_1 = b_2$ therefore g is one-to-one. $\square$

(e)

Show that $g \circ f$ is onto and g is one-to-one $\Longrightarrow$ f is onto.

Proof. Assume that $g \circ f$ is onto and g is one-to-one. We want to show that for all $b \in B$, there exists $a \in A$ such that $f(a) = b$. Let $b \in B$ be arbitrary, thus $g(b) \in C$. Since $g \circ f$ is onto, this means that there exists $a \in A$ such that $g(f(a)) = c$. Since g is one-to-one and $c = g(f(a)) = g(b)$, this means that $f(a) = b$. Thus for all $b \in B$, there exists $a \in A$ such that $f(a) = b$. $\square$

2.3

(4) 2.3.1

Prove that

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6} \qquad \forall n \in \mathbb{N}$$

Proof. We must show the base case and the inductive step in order to show that the statement holds for all natural numbers.

$\boxed{\text{Base Case}}$ Let $n = 1$, then

$$1^2 = \frac{1(1+1)(2(1)+1)}{6}$$

This holds.

$\boxed{\text{Inductive Step}}$ We want to show that if the equation holds for n, then it will hold for $n + 1$. Assume that

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

Then, adding $(n+1)^2$ to both sides we get

$$\begin{aligned}
1^2 + 2^2 + \cdots + n^2 + (n+1)^2 &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\
&= \frac{n(n+1)(2n+1) + 6(n+1)^2}{6} \\
&= \frac{(2n^3 + 3n^2 + n) + (6n^2 + 12n + 6)}{6} \\
&= \frac{2n^3 + 9n^2 + 11n + 6}{6} \\
&= \frac{(n+1)(n+2)(2(n+1)+1)}{6}
\end{aligned}$$

Thus, the statement is true for all $n \in \mathbb{N}$. $\square$

(5) 2.3.18

Let $a, b \in \mathbb{Z}$ such that $\gcd(a, b) = 1$. Let $r, s \in \mathbb{Z}$ such that $ar + bs = 1$. Show that $\gcd(a, s) = \gcd(b, r) = \gcd(r, s) = 1$.

Proof. Suppose that a and s have a commmon divisor that is not 1 or 0, call it p. Then there are integers q_a, q_s such that $a = pq_a$ and $s = pq_s$. It follows that

$$\begin{aligned}
ar + bs &= 1 \\
p(q_a r + bq_s) &= 1 \\
q_a r + bq_s &= \frac{1}{p}
\end{aligned}$$

The left hand side must be an integer, but the right hand side must be a fraction. Therefore they do not have a common divisor, and $\gcd(a, s) = 1$

We make the same argument for each other pair, so suppose $p \neq 1 \in \mathbb{Z}|r, b$, such that $b = pq_b$ and $r = pq_r$. Then we have

$$aq_r + q_b s = \frac{1}{p}$$

Which once again cannot be true becuase the LHS is an integer and the RHS is not. Therefore $\gcd(r, b) = 1$.

Similarly, suppose $p|r, s$ where $r = pq_r$ and $s = pq_s$. We get

$$aq_r + bq_s = \frac{1}{p}$$

As before, a contradiction arises in that this cannot have solutions where $p \neq 1$. Therefore $\gcd(r, s) = 1$. $\square$

3.4

(6) 3.4.1

(a)

For what x is $3x \equiv 2 \pmod{7}$?

Since $(5)3 = 15 = 14 + 1 = (2)7 + 1$, we say that $(5)3 \equiv 1 \pmod{7}$. So if we mutliply both sides by 5 we get

$$\begin{aligned} 3x &\equiv 2 \\ (5)3x &\equiv (5)2 \\ x &\equiv 10 \equiv 3 \end{aligned}$$

So if $x \in [3]_7$ then the equivalence holds.

(b)

For what x is $5x + 1 \equiv 13 \pmod{23}$?

We write

$$5x \equiv 12 \pmod{23}$$

Then we need the inverse of 5 in $\mathbb{Z}_{23}$. To do this we compute the extended Euclidean algorithm

$$\begin{aligned} 23 &= 5(4) + 3 \\ 5 &= 3(1) + 2 \\ 3 &= 2(1) + 1 \\ 3 - 2 &= 1 \\ 3 - (5 - (3(1))) &= 1 \\ 5(1) + 3(2) &= 1 \\ 5(1) + (23 - 5(4))(2) &= 1 \\ 23(2) - 5(7) &= 1 \end{aligned}$$

So $2 \cdot 7 = 14 = 5^{-1} \pmod{23}$. Hence

$$\begin{aligned}
5x + 1 &\equiv 13 \\
5x &\equiv 12 \\
(14)5x &\equiv (14)12 \\
x &\equiv 168 \\
x &\equiv (7)23 + 7 \\
x &\equiv 7
\end{aligned}$$

Therefore if $x \in [7]_{23}$ then x is a solution.

(c)

For what x is $5x + 1 \equiv 13 \pmod{26}$?

We must of course find $5^{-1} \pmod{26}$. We will again compute the extended Euclidean algorithm.

$$\begin{aligned}
26 &= 5(5) + 1 \\
26(1) + 5(-5) &= 1
\end{aligned}$$

So the inverse of 5 is $1 \cdot -5 \equiv -5 \equiv 21 \pmod{26}$. Then,

$$\begin{aligned}
5x + 1 &\equiv 13 \\
5x &\equiv 12 \\
(21)5x &\equiv (21)12 \\
x &\equiv 252 \\
x &\equiv 18
\end{aligned}$$

So our solutions will be $x \in [18]_{26}$.

(7) 3.4.2

(a)

This multiplication table does not form a group, because there is no identity element. Although $a * g = g \forall g \in G, a * g \neq g * a$, hence a is not a proper identity.

(d)

This also does not form a group. Our only candidate for an inverse element would be a. The element d does not have an inverse element such that $d * d^{-1} = a$.

(8) 3.4.6

Create a multiplication table for $U(12)$. The integers that are co-prime to 12 are $\{1, 5, 7, 11\}$ and their respective equivalence classes. We now compute the multiplication table.

	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

(9) 3.4.6 (modified)

Create a multiplication for $U(10)$. The integers that are coprime to 10 are $\{1, 3, 7, 9\}$.

	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

(10) 3.4.8

Find two elements of $GL_2(\mathbb{R})$ where multiplication is not commutative. Let $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$. Then

$$AB = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} * \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$$

$$BA = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} * \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$$