Elementary Set Theory and Abstract Algebra for Programmers

Answers to exercises

1), **Assume that you have a proper definition for integers. Create a well-defined set of rational numbers.**

- Given $a, b \in \mathbb{Z}$ are properly defined. We can define a rational number as $\frac{a}{b}$, where $b \neq 0$.

Equivalence: $\forall a, b, a', b' \in \mathbb{Z}$, the rational number (a, b) is equivalent to (a', b') iff $ab' = ba'$.

Operations

sum $\Rightarrow$ $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$

product $\Rightarrow$ $\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$

Well defined: The set of rational numbers as defined $\Rightarrow \frac{a}{b} \in \mathbb{Q}$ should be closed under addition and multiplication. Given the operations defined previously we can see that the sum or product of rational numbers as defined is a rational number, therefore is well defined

2). **Define the subset relationship between integers, rational numbers, real numbers, and complex numbers.**

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

where: $\mathbb{Z}$ are integers
$\mathbb{Q}$ are rational numbers
$\mathbb{R}$ are real numbers

3), Define the relationship between the set of trancendental numbers and the set of complex numbers in terms of subsets. Is it a proper subset?

Trancendental numbers are those that are not algebraic, i.e. they cannot be the roots of a non-zero polynomial with rational coefficients. That said, all trancendental numbers are real numbers so if we term all trancendental numbers as $\mathbb{T}$ then $\mathbb{T} \subset \mathbb{R}$. Given that the complex numbers $\mathbb{C}$ contain the real numbers, then $\mathbb{T} \subseteq \mathbb{R} \subset \mathbb{C}$ therefore $\mathbb{T} \subseteq \mathbb{C}$.

A proper subset, A of B is one where $\forall a \in A$, $a \in B$ - every element of A is in B. Additionally, $\forall b \in B$ where $b \notin A$, i.e. there exists one element in B that isn't in A.

As the complex numbers contain both real and imaginary numbers, then $\mathbb{I}$ is a proper subset of $\mathbb{C}$.

4). Using the formal definition of equality, show that if two finite sets have a different cardinality, they cannot be equal.

For a given two sets A and B where B has a greater cardinality that A. There must exist at least one elemnt of B that is not in A. If

$A = B$ iff $A \subseteq B$ & $B \subseteq A$ then

by $B \nsubseteq A$ they cannot be equal.

5), Given $A = \{1,2,3\}$ and $B = \{x,y,z\}$, compute the cartesian product of $B \times A$.

	x	y	z
1	(x,1)	y,1	z,1
2	x,2	y,2	z,2
3	x,3	y,3	z,3

6), Compute the cartesian product of $\{1,2,3,4\}$ and $\{3,6,9,12\}$ (in that order). If you were to pick 4 particular ordered pairs from this, what arithmetic computation would that encode?

	1	2	3	4
3	(1,3)	(2,3)	(3,3)	(4,3)
6	(1,6)	(2,6)	(3,6)	(4,6)
9	(1,9)	(2,9)	(3,9)	(4,9)
12	(1,12)	(2,12)	(3,12)	(4,12)

Randomly picking some ordered pairs would imply multiplication i.e..

(1,3) (3,3) (4,3)

$\Downarrow$

1×3, 3×3, 4×3

7). Define a mapping (function) from integers $n \in$ 1, 2, 3, 4, 5, 6 to the set {even, odd}

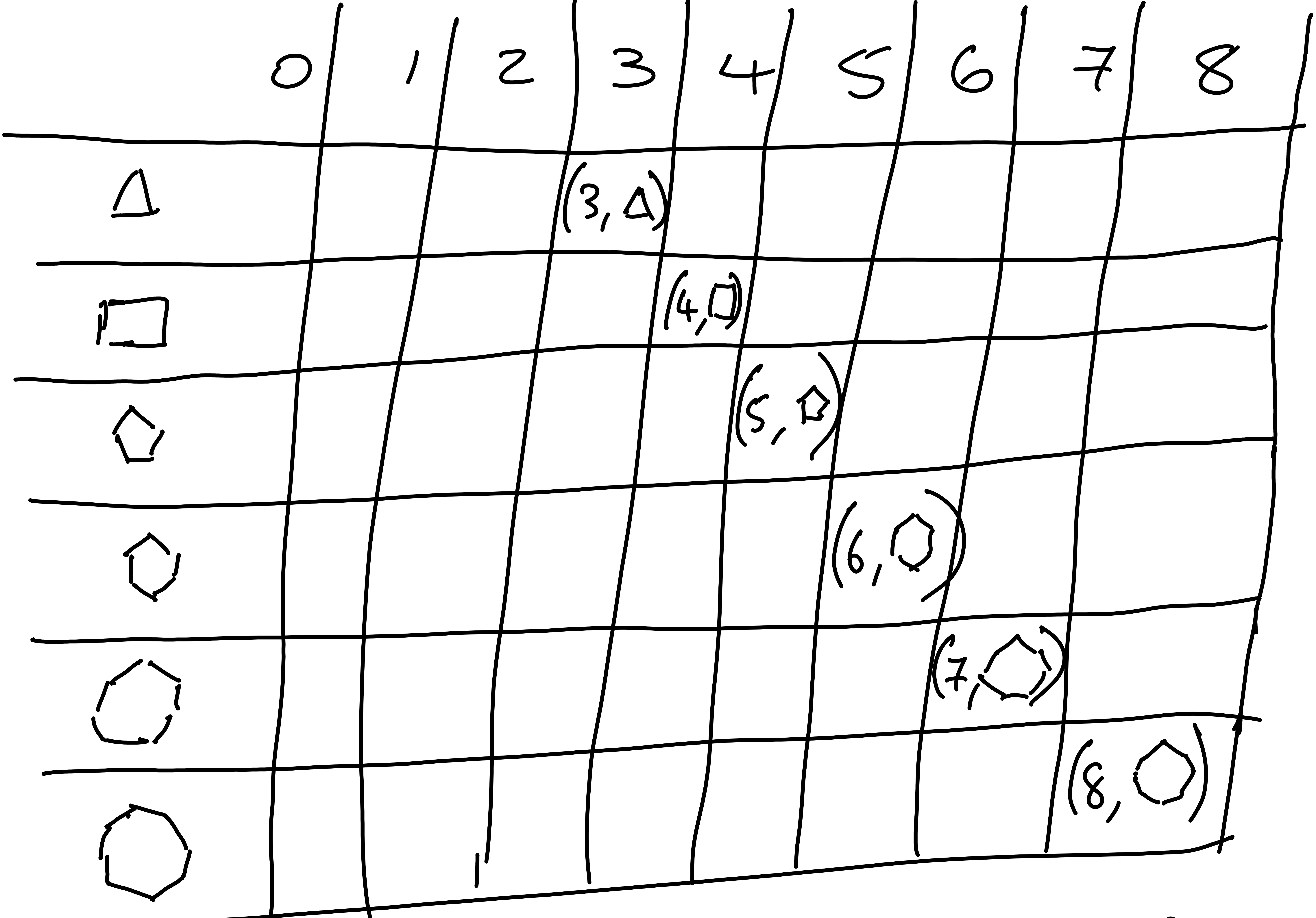
	1	2	3	4	5	6
even	X	(2, even)	X	(4, even)	X	(6, even)
odd	(1; odd)	X	(3, odd)	X	(5, odd)	X

This uses:

$$f(n) = \text{"even" iff } n \% 2 = 0$$
$$f(n) = \text{"odd" iff } n \% 2 \neq 0$$

8). Take the cartesian product of the set of integers 0, 1, 2, .., 8 and the polygons triangle, square, pentagon, hexagon, heptagon, and octogon.

Define a mapping such that the integer maps to the number of sides on the shape. For example, the ordered pair $(4, \square)$ should be in the subset, but $(7, \triangle)$ should not.



9), Define a mapping between positive integers and positive rational numbers.

It is possible to perfectly map the integers to rational number!

	1	2	3	4	5	6	7	8
1	1/1	2/1	3/1	4/1	5/1	6/1	7/1	8/1
2	1/2	2/2	3/2	4/2	5/2	6/2	7/2	8/2
3	1/3	2/3	3/3	4/3	5/2	6/3	7/3	8/3
4	1/4	2/4	3/4	4/4	5/4	6/4	7/4	8/4

As $\mathbb{Z} \subset \mathbb{R}$, all the integers can be mapped to rational numbers in this way. I.e. $1/1 = 1$, some elements are integers but that is also contained in the rational numbers. If we included 0 in our integer set, this would not be the case.

10), **Let set A be $\{1,2,3\}$ and set be $\{x, y, z\}$. Define a function from A to B that is well defined, but not surjective and not injective.**

We can define a piecewise function such that

$$f(n) = x \text{ if } n < 2$$
$$f(n) = y \text{ if } n \geq 2$$

It is not injective because x is mapped to twice. It is also not surjective because no element in A maps to z.

11), Pick a subset of ordered pairs that defines $a \times b \bmod 3$

	0	1	2
(0,0)	((0,0),0)		
(1,0)	((1,0),0)		
(2,0)	(2,0),0		
(0,1)	(0,1),0		
(1,1)		(1,1),1	
(2,1)			(2,1),2
(0,2)	(0,2),0		
(1,2)			(1,2),2
(2,2)		(2,2),1	

12), Given a relation between $(A \times A)$ and A: if the binary operator is commutative, then the map from $(A \times A)$ to A cannot be injective if the cardinality of the set is 2 or greater. Demonstrate the statement is correct by reasoning from $((a,b),c)$ and $((b,a),c)$ and the definition of injective

To be injective, $a,b \in A \times A$ and $c \in A$ so that $f(a,b) = f(c)$. However if $f(a,b)$ is commutative then

$$f(a,b) = f(c)$$
$$f(b,a) = f(c)$$

As a,b and b,a are different elements but map to the same element in the codomain then it cannot be injective.

13), Define our set A to be the numbers 0, 1, 2, 3, 4 and our binary operator to be subtraction modulo 5. Define all the ordered pairs of $A \times A$ in a table, then map that set of ordered pairs to A.

	0	1	2	3	4
0	0	4	3	2	1
1	1	0	4	3	2
2	2	1	0	4	3
3	3	2	1	0	4
4	4	3	2	1	0

14), Work out for yourself that concatenating "foo", "bar", "baz" in that order is associative.

Concatenation is preserving and closed so:

$$("foo" + "bar") + "baz" = "foobarbaz"$$

$$"foo" + ("bar" + "baz") = "foobarbaz"$$

15, Give an example of a magma and a semigroup. The magma must not be a semigroup.

Magma: The set of integers under the operation

$$f(a,b) = a.$$

This is closed but not associative

$$f(1,2) = 1$$

$$f(2,1) = 2$$

Semi group. The set of all natural numbers under the operation of the absolute value of the subtraction. $\forall a, b \in \mathbb{N}$

$$f \Rightarrow |a-b|$$

The absolute value insures this is closed but it is associative:

$$|20-6| = 14$$
$$|6-20| = 14$$

16), Let our binary operator be min(a,b) over integers. Is this a magma, semigroub or monoid. What is we restrict the domain to be positive integers (zero or greater)? What about the binary operator max(a,b) over those two domains

Given the set of $\mathbb{Z}$ and the operation

$$f(a,b) = \min(a,b)$$

Working backwards, it is not a monoid as ther is no integer e, such that

$$\min(a,e) =$$

It is a semigroup as

$$\min(a, \min(b,c)) = \min(\min(a,b), c)$$

And it is closed as every output is an integer. Thus it is a semigroup.

If we restrict the domain to positive integers (zero or greater) then 0 becomes the identity

$$\min(a,0) = 0$$

So it would then be a monoid

For the operator max(a,b) it is a semi group in both domains.

17), Let our set be all 3 bit binary numbers (a set of cardinality 8). Let our possible binary operators be the bitwise operators (and, or, xor, nor, xnor, and nand). Clearly this is closed because the output is a 3-bit binary number. For each binary operator, determine if the set under that binary operator is a magma, semigroup or monoid.

	Associative	Identity	Type
AND	YES	111	MONOID
OR	YES	000	MONOID
XOR	YES	000	MONOID
NOR	YES	NO, BECAUSE INVERSION	SEMIGROUP
XNOR	YES	⇑	SEMIGROUP
NAND	YES	⇑	SEMIGROUP

18), Why can't strings under concatenation be a group?

Because there is no inverse element for concatenation.

19), Polynomials under addition satisfy the property of a group. Demonstrate this is the case by showing it matches all the properties that define a group.

Closure: For two polynomials $a(x)$ and $b(x)$ the sum $a(x)+b(x)$ is also a polynomial

Assoccativity: For three polynomials $a(x), b(x)$ and $c(x)$

$$\big(a(x)+b(x)\big)+c(x) = a(x)+\big(b(x)+c(x)\big)$$

This is due to the coefficents being real numbers

Identity Element: The zero polynomial is the identity

$$a(x)+0 = 0+a(x) = a(x)$$

Inverse: For a polynomial $a(x)$, there always exists an inverse $-a(x)$ such that $a(x)+(-a(x)) = 0$