1. (a). The power set of \{a, b, c\} is 
Solution: \{\emptyset, \{a\}, \{b\}, \{a, b\}\}

(b). Verify that the set \(E\) of even integers is a countable set. 
(No need to verify that a function is 1-1 or onto here – I’ll trust you on this one.) 
Solution: Define \(f: \mathbb{Z}^+ \rightarrow E\) by 
\[ f(n) = \begin{cases} n & \text{n is even} \\ -n + 1 & \text{n is odd} \end{cases} \]
(There are other possibilities as well.)

2. (a). Explain why the table below cannot be completed to that of a semigroup. 
\[
| & a & b & c & d & e & f \\
- a & b \\
- b & c \\
- c & d \\
- d & e \\
- e & f \\
- f & a \\
\]

Solution: No matter how this table is extended, the resulting binary structure will not have any idempotents and hence cannot be a semigroup.

(b). The table below is that of a partially filled semigroup. 
What is the value of \(a \ast b\)?

\[
| & a & b & c & d \\
- a & a & d \\
- b & d \\
- c & b \\
- d & c \\
\]

Solution: \(a \ast b = a \ast (c \ast d) = (a \ast c) \ast d = d \ast d = c\)

(c). The table below is the partially filled table for a commutative group on 5 elements. Fill in the missing portions of the table.

\[
| & a & b & c & d & f \\
- a & a \\
- b & d & f \\
- c & \ \\
- d & \ \\
- f & \ \\
\]

\[
| & a & b & c & d & f \\
- a & a & b & c & d & f \\
- b & b & d & a & f & c \\
- c & c & a & f & b & d \\
- d & d & f & b & c & a \\
- f & f & c & d & a & b \\
\]
3. Let \( f : R \rightarrow R^* \) be defined by \( f(x) = e^x \), give the definition of an operation \( * \) on \( R \) so that \( f \) will be an isomorphism from \((R,*)\) to \((R^*,+)\).

What is the value of \( 0 * 0 \)?

Solution: Let \( a, b \in R \). Then \( f(a * b) = f(a) + f(b) \iff e^{a+b} = e^a + e^b \).

Hence, \( a * b = \ln(e^a + e^b) \). Thus \( 0 * 0 = \ln 2 \).

4. (a). Verify that \((Z,\ast)\) where \( a \ast b = a + b - 2 \) for all integers \( a \) and \( b \) is a group.

What is the identity element for this group and what is the inverse of 7?

Solution: First we show that \( \ast \) is associative. For suppose that \( a,b,c \in R \). Then
\[
(a \ast (b \ast c)) = a \ast ((b + c - 2) = a + (b + c - 2) - 2 = a + b + c - 4
\]
\[
(\ast (a \ast b) \ast c) = (a + b - 2) \ast c = a + b - 2 + c - 2 = a + b + c - 4
\]
Hence, \( a \ast (b \ast c) = (a \ast b) \ast c \).

The integer 2 is an identity since for any integer \( a \),
\[
a \ast 2 = a + 2 - 2 = a
\]
Each integer \( a \) has an inverse \( a' = 4 - a \) since
\[
a \ast (4 - a) = a + (4 - a) - 2 = 2
\]
In particular, the inverse of 7 is \(-3\).

(b). The binary structure \((R^* - \{1\},\circ)\) where \( x \circ y = x^{\ln y} \) for all \( x, y \) in \( R \), is a group (you do not need to verify this). What is the inverse of the number \( e^2 \)?

Solution: It is easy to see that the identity for this operation is the number \( e \).
For if \( a \) is any real number then \( a \circ e = a^{\ln e} = a^1 = a \) and \( e \circ a = e^{\ln a} = a \).
If \( x \) denotes the inverse of \( e^2 \), then \( e = x \circ e^2 = x^{\ln e^2} = x^2 \Rightarrow x = \sqrt{e} \).

5. Show that \( r = \sqrt{1 + \sqrt{2}} \) is not a rational number. You may use the fact that \( \sqrt{2} \) is not a rational number to determine a contradiction. You may also use the fact that the rational numbers are closed under addition and multiplication.

Hint: Begin with suppose that \( r = \sqrt{1 + \sqrt{2}} \) is a rational number, then

Proof. Suppose that \( \sqrt{1 + \sqrt{2}} \) is rational. Then \( \sqrt{1 + \sqrt{2}} = \frac{a}{b} \) for some integers \( a \) and \( b \). But then \( 1 + \sqrt{2} = \frac{a^2}{b^2} \Rightarrow \sqrt{2} = \frac{a^2 - b^2}{b^2} \in Q \) which is impossible since \( \sqrt{2} \) is irrational.
6. Fill in the requested details of the argument below.

**Theorem.** Let \( n \) and \( m \) be positive integers, and \( d = \gcd(n,m) \).
Then \( d \) is the smallest positive element of the set \( A = \{ an + bm : a, b \in \mathbb{Z} \} \).

**Proof.** We first note that \( A \) does contain some positive values since \( n \) must belong to \( A \) because \( \text{________} \).

Now we let \( d \) denote the least positive integer in \( A \). What is it that justifies the existence of \( d \)? The **Well-Ordering Principle**
Hence there exist integers \( a \) and \( b \) such that \( d = an + bm \).
We claim that \( d \) divides \( n \). If it did not then we could find integers \( q \) and \( r \) with
\[
 n = qd + r \text{ where } 0 < r < d \text{ (fill in the blank with appropriate bounds on } r.)
\]
But then we get that \( r = n - dq = n - q(an + bm) = (1 - qa)n + qbm \)
but this is a contradiction because this would imply that \( r \) belongs to \( A \) and yet \( r \) is a positive integer that is smaller than \( d \) – contrary to the choice of \( d \).
Thus \( d \) divides \( n \) and similarly \( d \) divides \( m \).

Now suppose that \( k \) is any other divisor of both \( n \) and \( m \), then \( n = kr, m = ks \) for some integers \( r \) and \( s \). And so now \( d = an + bm = \text{________} \)and so (explain how you know that \( k \) must be smaller than \( d \)).

this implies that \( k \) divides \( d \) and so \( k \leq d \).

Make sure that in the details above you have indicated clearly where it is that you used the fact that \( d \) was the smallest positive element of \( A \).

7. (a). How many commutative operations are there on a set with 5 elements?
   Explain your answer.

**Solution:** Look at the table for the operation. It has 25 entries. But once we have set the values in the upper 10 squares and the 5 diagonal squares, the remaining values are determined by commutativity. Thus there are just 15 squares to fill and we may use any of 5 values in each of these squares. Thus there are \( 5^{15} \) commutative operations.

(b). How many equivalence relations are there on the set \( S = \{ a, b, c \} \).
   Explain your answer.

**Solution:**
There is one equivalence relation for every way to partition \( S \) into non-empty sets. There are five partitions of \( S \) and hence there are five equivalence relations on \( S \).
8. Let \((G, \ast)\) be a group and \(b\) a fixed element of \(G\).
Define \(f: G \rightarrow G\) by \(f(x) = b \ast x\) for every \(x\) in \(G\).
Show that \(f\) is onto.

**Solution:**
To show that \(f\) is onto we must show that every element of \(G\) is a functional value.
So, let \(y\) be any element of \(G\). Let \(x = b' \ast y\). Then,
\[f(x) = b \ast x = b \ast (b' \ast y) = (b \ast b') \ast y = e \ast y = y\] (where \(e\) denotes the identity element).