1) Suppose that you have a set {monyet, burung, ular}. Define a binary operator that turns it into a group using set-theoretic definitions

We can define an operation Left such that $\forall a,b \in S$

a Left b = a

Closure: As the returned element is one of the arguements then by definition it is closed

Associativity:

(a Left b) Left c = a Left (b Left c)

Identity: Any element can act as the identity element

Inverse:

Every element is its own inverse.

2), Find a binary operator that is closed but not associative for real numbers.

We could define the difference of squares to be the operation

$$\forall a,b \in \mathbb{R} \quad a \; diff^2 \; b = a^2 - b^2.$$

This would be closed but not associative.

3), Let our set be real numbers.

Show a binary operator that is not closed.

A trivial non-closed operator would be one that uplifts to the complex plane i.e.

$\forall a, b \in \mathbb{R}$ a lift $b = a + bi$

4), What algebraic structure is all odd integers under multiplication? All even integers under addition?

Odd integers under multiplication form a semigroup as there is no identity element (no odd integer multiplied by another element gives 1.

Even integers under addition form a group. It is closed as the sum of two evens is always even. Additim is associative. (Assuming we include zero as an even number) it has an identity which is zero. Additionally, every element has an inverse which is just the negation of itself.

5), Let our group be 3x2 matrices of integers under addition. What is the identity and inverse? Can this be a cyclic group?

The identity is the zero matrix.
The inverse is just the same matrix but with negated values.
It is not cyclic because all 3x2 matrices cannot be generated from a single matrix.

6), **Demonstrate that**

$$n \pmod p, n = \ldots -2, -1, 0, 1, 2, \ldots$$

is a group under addition.

Closure:

$\forall a, b \in \mathbb{Z}$ then the result $(a+b) \bmod p$ will always be within 0 and p-1 so therefore closed.

Associativity:

As $\mathbb{Z}$ is associative under addition, therefore so is addition mod p

Identity: The identity is zero as in integer addition.

Inverse:

There exists an element b in $\mathbb{Z}$ such that $(a+b=0) \bmod p$.

This assumes that p is a positive integer greater than 1

7), Demonstriate that

$g^n \pmod p$, $n = \ldots, -2, -1, 0, 1, 2, \ldots$

where g and p are relatively prime is a group under multiplication. That is, given elements g^a, g^b, $g^a \times g^b$ is

in the group and the binary operator follows the group laws.

Closed:

$\forall a, b, g \in \mathbb{Z}$

$$(g^a \bmod p)(g^b \bmod p) = g^{(a+b)} \bmod p$$

Given that a+b are from $\mathbb{Z}$ then a+b is in the set.

Associativity:

Again this is implied from integer addition

Identity:

The identity is $g^0 \bmod p = 1 \bmod p$

Inverse:

$\forall a \in \mathbb{Z}$ there exists $b \in \mathbb{Z}$ such that $g^a \cdot g^b \bmod p = 1$

8), Both integers and polynomials with integer coefficients are rings. It is possible to define a homomorphism from integers to polynomials and polynomials, but it isn't the same transformation

For the homomorphism from integers to polynomials we can map the integer to a rank 1 polynomial i.e. if we define the transform as poly

$$\forall\, a \in \mathbb{Z} \mid \quad poly(a) = aX$$

For the opposite direction, we could envisage a transform where we sum the co-efficients of a polynomial to yield a single number. As a literal example $ax^4 + bx^3 + cx^2 + dx + e$ would yield $a+b+c+d+e$, given that the coefficients are $\mathbb{R}$, this would suffice.