Problem set (mandatory):

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

   (a) the group has an identity element

   (b) for any element a in the group there exists an inverse element a^{-1} such that $a * a^{-1} = a^{-1} * a = e$

   (c) the binary operator is associative ie $(a * b) * c = a * (b * c)$

   (d) the group is closed under the binary operator ie $a * b$ is in the group

   to find such an operator we first need to define an identity element. let that be "monyet". TODO

2. Find a binary operator that is closed but not associative for real numbers. exponentiation ie for $a, b \in \mathbb{R} : a^b \in \mathbb{R}$ is not associative for real numbers.

3. Let our set be real numbers. Show a binary operator that is not closed. the binary operator $\sqrt{a}$ is not closed because for $a \in -\mathbb{R}$

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

   (a) odd integers under multiplication is not closed, associative, has identity element 1.

   (b) a semigroup is a set with a binary operator that is associative and closed(you cannot get an uneven number from the addition of two even numbers)

5. Let our group be 3×2 matrices of integers under addition. What is the identity and inverse? Can this be a cyclic group, why or why not? (Pay very close attention to the definition of cyclic group)

   (a) The identity is the zero matrix of shape 3x2

   (b) The inverse of any matrix A is -A

   (c) This cannot be a cyclic group because it is not generated by a single element. The group is infinite and has multiple generators.

6. Demonstrate that

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

   is a group under addition. Remember, you need to show that:

   - the binary operator is closed
   - the binary operator is associative
   - an identity exists

- every element has an inverse

(a) Closure: For any $a, b \in \mathbb{Z}/p\mathbb{Z}$, $(a + b) \bmod p$ is also in $\mathbb{Z}/p\mathbb{Z}$. This is because the result of $(a + b) \bmod p$ will always be in the range $[0, p - 1]$, which are precisely the elements of our group.

(b) The binary operator is associative as addition is associative

(c) The identity is 0

(d) The inverse of an element a is $-a \bmod p$ or equivalently $(p-a) \bmod p$

7. Demonstrate that

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

Where g and p are relatively prime is a group under multiplication. That is, given elements g^a, g^b, $(g^a) * (g^b)$ is in the group and the binary operator follows the group laws.

we need to show

(a) the binary operator is closed: Let $g^a \bmod p$ and $g^b \bmod p$ be any two elements in the group. Their product is $(g^a \bmod p) \cdot (g^b \bmod p) \bmod p = g^{a+b} \bmod p$. Since $g^{a+b} \bmod p$ is of the form $g^n \bmod p$ for some integer n, it is also an element of the group. Therefore, the binary operator is closed.

(b) the binary operator is associative as $g^{a+b} = g^a * g^b$

(c) an identity exists as $g^0 = 1$

(d) every element has an inverse as $g^{-a} = \frac{1}{g^a}$

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