Problem sheet 2

1. (a) The multiplication table of $\mathbb{Z}/3\mathbb{Z}$ is:

$$\begin{array}{c|c|c|c} \cdot & 0 & 1 & 2 \\ \hline 0 & 0 & 0 & 0 \\ \hline 1 & 0 & 1 & 2 \\ \hline 2 & 0 & 2 & 1 \end{array}$$

We check the properties of group:

- The operation (here the product), when applied to two elements of $\mathbb{Z}/3\mathbb{Z} \setminus \{0\}$, returns an element of $\mathbb{Z}/3\mathbb{Z} \setminus \{0\}$. Why did we check this? Because in the definition of group, the operation has to take two elements of G and return an element of G.
- The product is associative: You can either argue that it is because it comes from the product in $\mathbb{Z}$, which is associative (it is actually the product in $\mathbb{Z}$, and then we compute the remainder on the result), or you can look at all possibilities (since $\mathbb{Z}/3\mathbb{Z} \setminus \{0\}$ has only 2 elements it is still doable by hand).
- There is an element $e \in \mathbb{Z}/3\mathbb{Z} \setminus \{0\}$ such that for every $a \in \mathbb{Z}/3\mathbb{Z} \setminus \{0\}$, $e \cdot a = a \cdot e = a$. Looking at the part of the multiplication table that is about $\mathbb{Z}/3\mathbb{Z} \setminus \{0\}$, we see that we can take $e = 1$.
- For every $a \in \mathbb{Z}/3\mathbb{Z} \setminus \{0\}$ there is $b \in \mathbb{Z}/3\mathbb{Z} \setminus \{0\}$ such that $a \cdot b = b \cdot a = e$. Since $e = 1$, another look at the table tells us that we should take:
When $a = 1$, $b = 1$, and when $a = 2$, $b = 2$.

We have checked all the properties, so it is a group.

(b) It is not a group. Already the product of two elements of $\mathbb{Z}/4\mathbb{Z} \setminus \{0\}$ is not in $\mathbb{Z}/4\mathbb{Z} \setminus \{0\}$, since $2 \cdot 2 = 0$.

2. We want to show that $(a^{-1})^2$ is the inverse of a^2. To do this we compute both products $(a^{-1})^2 \cdot a^2$ and $a^2 \cdot (a^{-1})^2$ and check that we get e in both cases. We do the first one, the other is left to you:

$$(a^{-1})^2 \cdot a^2 = a^{-1} \underbrace{a^{-1} a}_{e} a = a^{-1} e a = a^{-1} a = e.$$

3. (a) We first multiply both sides of the equality **on the left** by a^{-1}, and get:

$$a^{-1}axb = a^{-1}c, \text{ so } xb = a^{-1}c \text{ since } a^{-1}a = e.$$

NOTE that it would be (in general) false to write $xb = ca^{-1}$, because we might not have $a^{-1}c = ca^{-1}$. The first operation, multiplying both sides on the left by a^{-1} preserves the equality because we do the same thing to both sides. To obtain $xb = ca^{-1}$ you would need to multiply the left hand side on the left by a^{-1} and the right hand side on the right by a^{-1}, which is not the same thing, so might not preserve the equality.

From $xb = a^{-1}c$ we multiply both sides on the right by b^{-1} and get

$$xbb^{-1} = a^{-1}cb^{-1}, \text{ so } x = a^{-1}cb^{-1}, \text{ since } bb^{-1} = e.$$

(b) We want to put all the x on the right, using that $xy = yx^2$ (we will see examples of groups where similar properties hold, for well-chosen x and y):

$$xyxy = xy(xy) = xyyx^2 = yx^2yx^2 = yxxyx^2 = yx(xy)x^2$$

$$= yxyx^2x^2 = y(xy)x^4 = yyx^2x^4 = y^2x^6.$$

4. $g^{mk} = (g^k)^m = e^m = e$.