Homework 2.

1) For each operation $*$ defined on a set below, determine whether or not $*$ gives a group structure on the set. If it doesn't, say which axioms fail to hold:

1. Define $*$ on $\mathbb{Z}$ by $a * b = |ab|$.
2. Define $*$ on $\mathbb{Z}$ by $a * b = \max\{a, b\}$.
3. Define $*$ on $\mathbb{Z}$ by $a * b = a + b + 1$.
4. Define $*$ on $\mathbb{Z}$ by $a * b = ab + b$.
5. Define $*$ on $\mathbb{Z}$ by $a * b = a + ab + b$.

<u>Solution.</u> **Do it.**

2) Let G be a group such that $g^2 = e$ for all $g \in G$. Then, G must be Abelian.
<u>Solution.</u> Let g_1 and g_2 be two elements of G. Then we must have

$$(g_1 g_2)^2 = g_1 g_2 g_1 g_2 = e. \tag{1}$$

Now, since $g^2 = e$ for all $g \in G$, we have that $g = g^{-1}$ for all g. From this and equation (1) we get $g_1 g_2 = g_2 g_1$, which shows that G is Abelian.

3) Show that if the order of a group G is an even integer, then, it must exist an element $x \in G$ such that $x \neq e$ and $x^2 = e$.
<u>Solution.</u> Assume the opposite. Then, we can pair every element of G with its inverse and we obtain

$$G = \{1, g_1, g_1^{-1}, ..., g_n, g_n^{-1}\}.$$

We can immediately see that in this case $|G| = 2n + 1$, which contradicts our assumption of even order for G. So, if we want G to have even order we have to add an element g such that $g = g^{-1}$, i.e. $|g| = 2$.

4) Let G be any group. Prove that its center $\mathcal{Z}(G)$ is a subgroup.

If $C(g)$ is the *centralizer* of $g \in G$, prove that

$$\mathcal{Z}(G) = \bigcap_{g \in G} C(g).$$

<u>Solution.</u> Recall that the definition of the *center* of the group G is

$$\mathcal{Z}(G) = \{g \in G \ : \ gx = xg \ \ \forall \ \ x \in G\}.$$

Now, we will show that this is a subgroup. First, because $ex = xe$ for all $x \ \in G$, we have $e \ \in \mathcal{Z}(G))$. Second, suppose that $g, \ h \ \in \mathcal{Z}(G)$, so that $gx = xg$ and $hx = xh$ for all $x \ \in G$. Then $(gh)x = g(hx) = g(xh) = (gx)h = (xg)h = x(gh)$, which shows that $gh \ \in \mathcal{Z}(G)$. Third, if $g \ \in \mathcal{Z}(G)$, then $gx = xg$ for every $x \ \in G$. Multiply this equation on both the left and the right by g^{-1}, and the resulting equation is $xg^{-1} = g^{-1}x$ for every $x \ \in G$. This shows that $x^{-1} \ \in \mathcal{Z}(G)$, showing that the inverse of every element in $\mathcal{Z}(G)$ is also in $\mathcal{Z}(G)$. These three properties show that $\mathcal{Z}(G)$ is a subgroup of G.

The second question needs only the definition of the centralizer $C(g)$ of $g \in G$. Do it by yourself.

5) Let G be the set

$$G = \left\{ \begin{pmatrix} 1 & y & x \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}, \quad x, \, y, \, z \, \in \mathbb{R} \right\}$$

Prove that G is a non-Abelian group (it is called the *Heisenberg* group) under matrix multiplication. Find its center.
<u>Solution.</u> **Do it.**

6) Let $H = 6\mathbb{Z}$ be a subgroup of $\mathbb{Z}$. Write down the quotient space $\mathbb{Z}/H$. Do the same if $H = \langle [4] \rangle$ in $\mathbb{Z}_{12}$.
<u>Solution.</u> We solved it in class.

7) If G is a group such that $(a \cdot b)^2 = a^2 \cdot b^2$ for all $a, \ b \in G$, show that G must be Abelian.
<u>Solution.</u> Let $a, \, b \in G$. Then, $(ab)^2 = a^2 b^2$, but by definition $(ab)^2 = abab$. Therefore, we have $abab = a^2 b^2$. Cancel a factor of a on the left and a factor

of b on the right, and we get $ba = ab$, which shows that G is Abelian.

8) In $GL(2, \mathbb{R})$, find the order of the following elements:

1. $\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$
2. $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

Solution. **Do it.**

9) Find all elements of finite order of the group $\mathbb{R}^\times$ and of the group $\mathbb{C}^\times$.
Solution. **Do it.**

10) Let c a positive constant. Show that the set L defined as

$$L = \left\{ A(v) := \left(1 - \frac{v^2}{c^2}\right)^{-1/2} \begin{pmatrix} 1 & -v \\ -\frac{v}{c^2} & 1 \end{pmatrix}, \quad v \in \mathbb{R},\ |v| < c \right\}$$

is a subgroup of $GL(2, \mathbb{R})$. Verify that $A(v_1)A(v_2) = A(v_3)$ where

$$v_3 = \frac{v_1 + v_2}{1 + \frac{v_1 v_2}{c^2}}.$$

The group L is the **Lorentz** group of Einstein's Special Relativity. If c is the speed of light what happens if we assume that $c = \infty$?
Solution. **Do it.**

11) Let

$$G = \left\{ \begin{pmatrix} \cos x & \sin x \\ -\sin x & \cos x \end{pmatrix} \;\middle|\; x \in \mathbb{R}, \right\}$$

Show that G is a group with group operation the matrix multiplication.

Solution. **Do it.**

12) If A and B are subgroups of G, show that $A \cap B$ is a subgroup of G.
Solution. **Do it.**

13) Consider the set

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

equipped with multiplication given by the relations:

$$1g = g1 = g, \ \ (-h)g = -hg, \ \ \forall\, g \in Q_8$$

$$ij = k, \ \ jk = i, \ \ ki = j, \ \ ji = -k, \ \ kj = -i, \ \ ik = -j$$
$$i^2 = j^2 = k^2 = -1$$

Check that Q_8 is a non-Abelian group of order 8. (It is called *the quaternion group*). Write all subgroups.
Solution. Solved in class.

14) Give an example of a subgroup H of a group G and of an element $g \in G$ such that $gHg^{-1} \subseteq H$, but $gHg^{-1} \neq H$.
Solution. Take $G = GL(2, \mathbb{Q})$ and let

$$H = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \,\middle|\, n \in \mathbb{Z} \right\}.$$

Take

$$g = \begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix}$$

Now,

$$g \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} g^{-1} = \begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix}^{-1} =$$
$$= \begin{pmatrix} 5 & 5n \\ 0 & 1 \end{pmatrix} \frac{1}{5} \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix} = \begin{pmatrix} 5 & 5n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 5^{-1} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 5n \\ 0 & 1 \end{pmatrix}$$

So, $gHg^{-1} \subseteq H$, but $gHg^{-1} \neq H$. The element

$$\begin{pmatrix} 1 & 6 \\ 0 & 1 \end{pmatrix} \in H$$

does not belong to gHg^{-1}.

ADDITIONAL EXERCISES.

15) Suppose that G is a subgroup of $\mathbb{Z}$. Then, there is a non-negative integer k such that $G = k\mathbb{Z}$.

Solution. Since G is a subgroup of $\mathbb{Z}$ we must have $0 \in G$. For the same reason, if g_1 and g_2 are in G, then $n_1 g_1 + n_2 g_2 \in G$.
Now, if $G \neq \{0\}$, it must contain a positive integer. Let k be the smallest positive integer in G. Take any $g \in G$. Then, for this g we have $g = nk + r$ with $0 \leq r < k$. But $nk \in G$ and therefore $r \in G$. But $r < k$, so r must be 0. Hence, $G = k\mathbb{Z}$.

15) Find the last decimal digit of 7^{222}.

Solution. In other words we want to find $7^{222} \pmod{10}$. Note that 7 and 10 are relatively prime, and $\varphi(10) = 4$. So by Fermat's theorem we get $7^4 \equiv 1 \pmod{10}$, i.e.

$$7^{222} \equiv 7^{4\times 55+2} \equiv (7^4)^{55} \times 7^2 \equiv 1^{55} \times 7^2 \equiv 49 \equiv 9 \pmod{10}.$$

16) Find the remainder of the division $\frac{50^{250}}{83}$.

Solution. First, we notice that $(83, 50) = 1$, so Fermat's theorem says

$$50^{82} = 1 \pmod{83}.$$

Now $3 \cdot 82 = 246$, so

$$50^{250} = 50^{246} \cdot 50^4 = (50^{82})^3 \cdot 2500^2 = 1^3 \cdot 10^2 = 100 = 17 \pmod{83}.$$

Remark. Another way is, first, to calculate 50^{250} (!!!) Using a computer (and not a calculator!) we find that this is equal to

52714787526044456024726519219225572551424023323922008641517022
09078987540239533171017648022222644649987502681255357847020768
63325972445883937922417317167855799198150634765625000000000000
00000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000.

Now you must divide the above number by 83 to find the remainder(!!)