University of California at San Diego – Department of Physics – Prof. John McGreevy

Physics 220 Symmetries Fall 2024
Assignment 1 – Solutions

Due 3:30pm Thursday, October 3, 2024

- Homework will be handed in electronically. Please do not hand in photographs of hand-written work. The preferred option is to typeset your homework. It is easy to do and you need to do it anyway as a practicing scientist. A LaTeX template file with some relevant examples is provided here, and the texfile with the problems below is on the homework page. If you need help getting set up or have any other questions please email me.
- To hand in your homework, please submit a pdf file through the course's Canvas website, under the assignment labelled hw01.

Thanks in advance for following these guidelines. Please ask me by email if you have any trouble.

---

1. **Brain-warmer.** Consider the group made from the set $\{2, 4, 6, 8\}$ under multiplication modulo 10.

   (a) Write the multiplication table and check the sudoku rule. What is the identity?

	2	4	6	8
2	4	8	2	6
4	8	6	4	2
6	2	4	6	8
8	6	2	8	4

   The identity is 6!

   (b) Is it equivalent to $\{1, 2, 3, 4\}$ under multiplication modulo 5? If not, why not?

   It is not the *same* as this group, since the multiplication table for the latter is

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

which looks quite different (in particular the identity for this group is 1). However, both of these groups are isomorphic to $\mathbb{Z}_4$, as we can see by noticing that each has elements of order 4 (for example, 2 in both cases), which generates a $\mathbb{Z}_4$ subgroup, which is therefore the whole group.

Since there are only 4 elements, the group isomorphism is easy enough to describe:

$$1 \to 6, 2 \to 2, 3 \to 8, 4 \to 4$$

2. **A more economical definition of group.** Show that we can weaken two of the conditions defining a group without changing the outcome, as follows:

   (2') A left identity $\mathbb{1}$ exists, such that for any element g, $\mathbb{1}g = g$.

   (3') For any element g, a left inverse f exists: $fg = \mathbb{1}$.

   Show that these two conditions imply that the left identity is also the right identity and the left inverse is also the right inverse.

   Consider f, the left inverse of g. The condition (3') says that there exists a left inverse of f – another element k with

   $$kf = \mathbb{1}.$$

   Now multiply the BHS of this equation on the right with g:

   $$(kf)g = \mathbb{1}g = g = k(fg) = k\mathbb{1}.$$

   We used associativity.

   To see that g is k, multiply both sides of $g = k\mathbb{1}$ by $\mathbb{1}$ on the right:

   $$g\mathbb{1} = k\mathbb{1}\mathbb{1} = k\mathbb{1} = g.$$

   Therefore $g\mathbb{1} = g$ for any g, so $\mathbb{1}$ is also the right identity. But then the equation $g = k\mathbb{1}$ says $g = k$.

3. **The group with three elements.** Write down the multiplication table for the group with three elements; show that it is uniquely fixed by the definition. Is it abelian?

   Well, one element is the identity e. Call the second element g. The third element must be the inverse of g, g^{-1}. It is both the left and right inverse. Therefore the group is abelian. Therefore the multiplication table is

   $$\begin{array}{cc} & \begin{array}{ccc} e & g & g^{-1} \end{array} \\ \begin{array}{c} e \\ g \\ g^{-1} \end{array} & \begin{bmatrix} e & g & g^{-1} \\ g & g^2 & g^{-1}g = e \\ g^{-1} & gg^{-1} = e & g^{-2} \end{bmatrix} \end{array}$$

Who are g^2 and its inverse g^{-2}? We've run out of elements, so it must be one of e, g, g^{-1}. But the requirement that every element has an inverse means that every element must appear once in each row and column of the table. Therefore $g^2 = g^{-1}$. This group is called $\mathbb{Z}_3$, and has a nice one-dimensional representation in terms of the cube roots of unity, where

$$D(e) = 1, D(g) = \omega, D(g^{-1}) = \omega^2, \quad \omega \equiv e^{2\pi \mathbf{i}/3}.$$

4. **Groups with four elements.** Write down the multiplication table for all groups with four elements. Are they all abelian?

One way to do it is following the logic of the previous problem.

	e	a	b	c
e	e	a	b	c
a	a	a^2	ab	ac
b	b	ba	b^2	bc
c	c	ca	cb	c^2

The elements $a^2, ab...$ must all come from the set $\{e, a, b, c\}$. Consider a^2. Up to relabelling $b \leftrightarrow c$, there are two possibilities: either it is e or it is b. Suppose first it is $a^2 e$. Then the rest of the a column and row are fixed by sudoku rule:

	e	a	b	c
e	e	a	b	c
a	a	a^2	c	b
b	b	c	b^2	bc
c	c	b	cb	c^2

Now it looks like there are two possibilities for the bottom right block, namely $\begin{pmatrix} e & a \\ a & e \end{pmatrix}$ or $\begin{pmatrix} a & e \\ e & a \end{pmatrix}$. But these two possibilities are related by the relabelling $b \to c$. Either one is the group $\mathbb{Z}_2 \times \mathbb{Z}_2$:

$\mathbb{Z}_2 \times \mathbb{Z}_2$	e	a	b	c
e	e	a	b	c
a	a	a^2	c	b
b	b	c	e	a
c	c	b	a	e

Now go back to the possibility that $a^2 = b$:

$$\begin{array}{c|cccc} & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & b & ab & cb \\ b & b & ba & b^2 & bc \\ c & c & ca & cb & c^2 \end{array}$$

Can we have $ab = e$? No because then we would need $cb = c$ which means $b \stackrel{?}{=} e$, we lose a group element. So $ab = c$. The same logic applies to ba (and therefore the group is abelian). This gives:

$$\begin{array}{c|cccc} & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & b & c & e \\ b & b & c & b^2 & bc \\ c & c & e & cb & c^2 \end{array}$$

Can we have $b^2 = a$? No because multiplying the BHS on the left by a gives $ab^2 = a^2 = b$ which means $ab \stackrel{?}{=} e$, which is false. Therefore, we must have $b^2 = e$ and we are done:

$$\begin{array}{c|cccc} \mathbb{Z}_4 & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & b & c & e \\ b & b & c & e & a \\ c & c & e & a & b \end{array}$$

– which is the group $\mathbb{Z}_4$.

Perhaps less arduous is to note that by Lagrange's theorem, the orders of the elements must divide the order of the group, so every element other than the identity must be order 2 or order 4. If there is an element of order 4, then its powers account for all the elements and the group is just $\mathbb{Z}_4 = \langle a | a^4 = e \rangle$. If there is an element of order 2 (but not an element of order 4), there must be three of them. This is $\mathbb{Z}_2^2 = \langle a, b | a^2 = e, b^2 = e, ab = ba \rangle$. (These relations imply that $(ab)^2 = e$ as well.)

An elementary statement (I learned from Yu-Hsueh Chen's solution) that makes clear that there are only two possibilities is to consider which elements are each others' inverses. There are in fact only two possibilities for the answer: $\{1, f, f^{-1}, g\}$ with $g^{-1} = g$ and $\{1, f, g, h\}$ with each element its own inverse. This information determines the whole table in each case by the sudoku rule.