Math Circles. Group Theory. Solution Set 2.

Diana Carolina Castañeda Santos
dccastan@uwaterloo.ca
University of Waterloo

March 27, 2019

Solutions:

1. Find all the elements of $(\mathbb{Z}_{12}^*, \cdot)$ and draw out the multiplication table for this group.

   The elements in $\mathbb{Z}_{12}^*$ are the units in $\mathbb{Z}_{12}$. These are the numbers that don't have common divisors with 12. These are 1, 5, 7, and 11. The multiplication table is:

$\cdot$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

2. Find all values of x in $\mathbb{Z}_{10}$ that satisfy the equation $3x + 9 = 1 \pmod{10}$.

$$\begin{aligned} 3x + 9 &= 1 \pmod{10} \\ 3x &= -8 \pmod{10} \\ 3x &= 2 \pmod{10} \end{aligned}$$

   We try all values of x from 0 to 9 and we see that $x = 4$ is the only solution to this equation.

3. Does the equation $x^2 = -1 \pmod 5$ have solutions in $(\mathbb{Z}_5^*, \cdot)$?

   We can replace x by the possible values that it could be in $\mathbb{Z}_5$.

x	0	1	2	3	4
x^2	0	1	4	4	1

   Recall that $-1 = 4 \pmod 5$. Hence $x = 2$ and $x = 3$ are the solutions of the equation.

4. Determine the order of the following groups:

   (a) $|D_5| = 10$.

   (b) $|(\mathbb{Z}_{12}, +)| = 12$.

   (c) $|(\mathbb{Z}_{12}^*, \cdot)| = 4$.

   (d) $|S_4| = 24$

   (e) $|(\mathbb{Z}_p^*, \cdot)| = p - 1$ where p is prime.

   (f) $|S_n| = n!$ where $n \in \mathbb{N}$

5. Determine the order of the following elements

   (a) $|i| = 4$ in $\mathcal{Q}_8$.

   (b) $|3| = 8$ in $(\mathbb{Z}_8, +)$.

   (c) $|3| = 2$ in $(\mathbb{Z}_8^*, \cdot)$.

   (d) $|a|$ for each a in $(\mathbb{Z}_5^*, \cdot)$.

$$\begin{aligned} |1| &= 1 \\ |2| &= 4 \\ |3| &= 4 \\ |4| &= 2 \end{aligned}$$

   (e) $|HV| = |R^2| = 2$ in D_4.

6. Determine all the groups of order 4.

   There are only two non-isomorphic groups $(\mathbb{Z}_4, +)$ and $(\mathbb{Z}_8^*, \cdot)$.

7. Determine all groups of order 5.

   There is only one group of order 5 which is $(\mathbb{Z}_5, +)$.

8. Draw out the multiplication table of S_3.

$\cdot$	id	(132)	(123)	(12)	(13)	(23)
id	id	(132)	(123)	(12)	(13)	(23)
(132)	(132)	(123)	id	(23)	(12)	(13)
(123)	(123)	id	(132)	(13)	(23)	(12)
(12)	(12)	(13)	(23)	id	(132)	(123)
(13)	(13)	(23)	(12)	(123)	id	(132)
(23)	(23)	(12)	(13)	(132)	(123)	id

9. We know that D_3, S_3 and $(\mathbb{Z}_6, +)$ are groups of order 6. Are they isomorphic? are all of them non-isomorphic?

   Since D_3 and S_3 are not abelian, and $(\mathbb{Z}_6, +)$ is abelian, we can say that $(\mathbb{Z}_6, +)$ is not isomorphic to D_3 and S_3.

   To decide if D_3 and S_3 are isomorphic, we look at the multiplication tables. The multiplication table for S_3 was found in problem 8. Also, in the previous lesson we saw that the multiplication table for D_3 is:

$\cdot$	e	R	R^2	V	D	D'
e	e	R	R^2	V	D	D'
R	R	R^2	e	D'	V	D
R^2	R^2	e	R	D	D'	V
V	V	D	D'	e	R	R^2
D	D	D'	V	R^2	e	R
D'	D'	V	D	R	R^2	e

   Hence, if we rename: $e \leftrightarrow$ id, $R \leftrightarrow (132)$, $R^2 \leftrightarrow (123)$, $V \leftrightarrow (12)$, $D \leftrightarrow (13)$, and $D' \leftrightarrow (23)$. The two tables are the same. Thus D_3 is isomorphic to S_3.

10. Draw out the multiplication table of the group of quaternions $(\mathcal{Q}_8, \cdot)$.

$\cdot$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	j	$-j$
$-i$	$-i$	i	1	-1	$-k$	k	$-j$	j
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

11. Prove that inverses are unique. In other words, prove that if $ab = ba = e = ac = ca$ then $c = b$.

Proof. Since c is an inverse of a, we know $ac = e$. We can multiply this equation by the left by b and we see that

$$\begin{aligned} b(ac) &= b \cdot e \\ (ba)c &= b \cdot e \\ e \cdot c &= b \cdot e \\ c &= b. \end{aligned}$$

The second equation is possible by the associativity property. the third equation is true because b is inverse of a, and the last equation is possible because of the identity property. □