Math Circles. Group Theory. Solution Set 3.

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

April 3, 2019

Problems:

1. Determine all the groups of order 4.

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

2. Determine all groups of order 5.

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

3. 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

4. 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?

   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:

   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.

$\cdot$	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

5. Is $\{0, 5, -5\}$ a subgroup of $(\mathbb{Z}, +)$?

   It is not a subgroup, it doesn't have the closure property, for instance $5+5+5 = 15 \notin \{0, 5, -5\}$.

6. Find all the subgroups of S_3.

   The subgroups of S_3 are $\{\text{id}\}$, $\{\text{id}, (12)\}$, $\{\text{id}, (13)\}$, $\{\text{id}, (22)\}$, $\{\text{id}, (123), (132)\}$, and S_3.

7. What are the possible orders for a subgroup of $(\mathbb{Z}_{12}, +)$? For each order, can you find a subgroup of that order?

   The possible subgroup orders are the divisors of 12. It means, 1, 2, 3, 4, 6, and 12

$$\begin{aligned}
\text{Subgroup of order } 1 &: \{0\} \\
\text{Subgroup of order } 2 &: \{0, 6\} \\
\text{Subgroup of order } 3 &: \{0, 4, 8\} \\
\text{Subgroup of order } 4 &: \{0, 3, 9\} \\
\text{Subgroup of order } 6 &: \{0, 2, 4, 6, 8, 10\} \\
\text{Subgroup of order } 12 &: \mathbb{Z}_{12}
\end{aligned}$$

8. Prove that the order of an element divides the order of the group.

   Let $a \in G$ of order $|a| = n$. Consider the set $\{e, a, a^2, \cdots a^{n-1}\}$. You can verify that this is a group. In fact it is a subgroup of G. Then, by Lagrange's theorem the order of this subgroup divides $|G|$, and this subgroup has precisely $|a|$ elements. Thus $|a|$ divides $|G|$.

9. Find all the subgroups of D_4 (The group of symmetries of the square).

   D_4 has 10 subgroups. $\{e\}$, $\{e, H\}$, $\{e, V\}$, $\{e, D\}$, $\{e, D'\}$, $\{e, R, R^2, R^3\}$, $\{e, R^2\}$, $\{e, H, V, R^2\}$, $\{e, D, D', R^2\}$, D_4

10. 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. □