ES.S20: Group Theory

Worksheet #3

Problem #1

(i) Write down one example of a group of order 7.

(ii) Show that all groups of order 7 are identical with the one you wrote down in **(i)**.

(i) Let x denote a rotation through $2\pi/7$ radians of a seven-spoked wheel, for example. $x^7 = 1$ as seven of these rotations take the wheel back to its initial position. Let G denote the group of rotations given by all powers of x. G is the group generated by x: $G = \langle x \,|\, 1, x, x^2, \ldots, x^7 = 1\rangle = \langle x \rangle$. So, $G = \langle x \rangle$ is cyclic.

(ii) Take H to be a group of order $|H| = 7$. Choose $a \in H$ with $a \neq 1$. Then $o(a) \,\Big|\, |H| = 7$. So, $o(a) = 7$ since $a \neq 1$ and the only divisors of 7 are 1 and 7. It follows that $o(a) \neq 1$. Hence the subgroup $\langle 1, a, a^2, \ldots, a^6 \rangle$ is cyclic of order 7 and lies in H. So, this group is the whole of $H = \langle a \,|\, 1, a, a^2, \ldots, a^6, a^7 = 1\rangle$ and H is cyclic of order 7. So, any group of order 7 is cyclic of order 7 and is isomorphic to $G = \langle x \,|\, x^7 = 1\rangle$ in **(i)**. That is, $a\theta = x$.

Problem #2

Can you generalize what you just did in **Problem #1**? Hint: Does this apply to more integers than just 7?

We could, for instance, replace 7 and 11 and try to generalize from there.

(i) This holds true for any prime p. $G = \langle x \,|\, x^p = 1\rangle$ where the element x denotes a rotation of $2\pi/7$ radians.

(ii) $|H| = p$. $o(a)$ for $a \in H$ is $o(a) = p$. So, $H = \langle a \,|\, a^p = 1\rangle$.

Problem #3

Write down all you currently know about groups of order $m \in \{1, 2, 3, 4, 5, 6, 7, 8\}$.

If $|G| = p$ and p is prime, apply the result of **Problem #2**: G is cyclic of order p. This deals with groups of order $m \in \{1, 2, 3, 5, 7\}$.

Suppose that the order of the group G is four: $|G| = 4$. We recognize that this is the Klein four-group: $\langle \iota, (1\,2)\,(3\,4), (1\,4)\,(2\,3), (1\,3)\,(2\,4)\rangle \cong \langle 1, a, b, c \,|\, a^2 = b^2 = c^2 = 1, ab = ba, \ldots \rangle$.

There is also a cyclic group of order 4: If we have a square and the element x denotes moving clockwise from one vertex to the next: That is, let x denote $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 4$, $4 \mapsto 1$. Then x^2 denotes $1 \mapsto 3$, $2 \mapsto 4$, $\dots$, and so on.

Suppose that $|G| = 6$. $S_3 = \{\iota, (1\,2\,3), (1\,3\,2), (1\,2), (1\,3), (2\,3)\}$ and is cyclic of order 6.

Suppose that $|G| = 8$. From the work we've already done, we have observed that Q (quaternions) and G are groups of order 8. We could look up some others as well — the dihedral group is a example.

Problem #4

Write out the multiplication table for $\mathbb{Z}_5$, where $\mathbb{Z}_5$ denotes the integers modulo 5 under addition. Next, write out the multiplication table for $\mathbb{Z}_5^*$, where $\mathbb{Z}_5^*$ denotes the non-zero integers modulo 5 under multiplication.

(i) Find an element of order 5 in $\mathbb{Z}_5$.

(ii) Find an element of order 4 in $\mathbb{Z}_5^*$.

The integers modulo 5 have five classes: $\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}$. For example, $\overline{0} = \{0, \pm 5, \pm 10, \dots\}$ and $\overline{1} = \{1, 6, 11, \dots\}$. Note that $\overline{x} + \overline{y} = \overline{x+y}$.

(i) $\overline{3}$ is of order 5. In fact, all non-zero elements are of 5 in $\mathbb{Z}_5$.

(ii) $\overline{4}$ is an element of order 4 in $\mathbb{Z}_5^*$. Check this out: $\overline{44} = \overline{16} = \overline{1}$ so $\overline{4444} = \overline{1}$.

$\mathbb{Z}_5$	$\overline{\mathbf{0}}$	$\overline{\mathbf{1}}$	$\overline{\mathbf{2}}$	$\overline{\mathbf{3}}$	$\overline{\mathbf{4}}$
$\overline{\mathbf{0}}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{\mathbf{1}}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{\mathbf{2}}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{\mathbf{3}}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{\mathbf{4}}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\mathbb{Z}_5^*$	$\overline{\mathbf{1}}$	$\overline{\mathbf{2}}$	$\overline{\mathbf{3}}$	$\overline{\mathbf{4}}$
$\overline{\mathbf{1}}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{\mathbf{2}}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{\mathbf{3}}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{\mathbf{4}}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$