Math 534 Homework 2

Morgan Gribbins

January 30, 2020

(1)

Write down the group table for $(\mathbb{Z}/4, +_4)$ and $((\mathbb{Z}/5)^\times, \times_5)$. Are they related? If so, explain how.

$\mathbb{Z}/4$	**0**	**1**	**2**	**3**
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$(\mathbb{Z}/5)^\times$	**1**	**2**	**3**	**4**
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

These groups are isometric under the mapping $\psi : \mathbb{Z}/4 \to (\mathbb{Z}/5)^\times$, with $\psi(0) = 1, \psi(1) = 4, \psi(2) = 2, \psi(3) = 3$.

(2)

For each of the following groups G, find $|G|$ and $|g|$ for every $g \in G$:

(a) $G = \mathbb{Z}/12$

$|0| = 1$, as $0 = e$.
$|1| = 12$, as $1+1+1+1+1+1+1+1+1+1+1+1 = 12 = 0 = e$.
$|2| = 6$, as $2+2+2+2+2+2 = 12 = 0 = e$.
$|3| = 4$, as $3+3+3+3 = 12 = 0 = e$.
$|4| = 3$, as $4+4+4 = 12 = 0 = e$.
$|5| = 12$, as $5+5+5+5+5+5+5+5+5+5+5+5 = 60 = 0 = e$.
$|6| = 2$, as $6+6 = 12 = 0 = e$.

$|7| = 12$, as $7+7+7+7+7+7+7+7+7+7+7+7 = 84 = 0 = e$.
$|8| = 3$, as $8+8+8 = 24 = 0 = e$.
$|9| = 4$, as $9+9+9+9 = 36 = 0 = e$.
$|10| = 6$, as $10+10+10+10+10+10 = 60 = 0 = e$.
$|11| = 12$, as $11+11+11+11+11+11+11+11+11+11+11+11 = 132 = 0 = e$.

(b) $G = (\mathbb{Z}/12)^{\times}$

$|1| = 1$, as $1 = e$.
$|5| = 2$, as $5 \times 5 = 24 = 1 = e$.
$|7| = 2$, as $7 \times 7 = 49 = 1 = e$.
$|11| = 2$, as $11 \times 11 = 121 = 1 = e$.

(c) $G = (\mathbb{Z}/16)^{\times}$

$|1| = 1$, as $1 = e$.
$|3| = 4$, as $3 \times 3 \times 3 \times 3 = 81 = 1 = e$.
$|5| = 4$, as $5 \times 5 \times 5 \times 5 = 625 = 1 = e$.
$|7| = 2$, as $7 \times 7 = 49 = 1 = e$.
$|9| = 2$, as $9 \times 9 = 81 = 1 = e$.
$|11| = 4$, as $11 \times 11 \times 11 times 11 = 14641 = 1 = e$.
$|13| = 4$, as $13 \times 13 \times 13 \times 13 = 28561 = 1 = e$.
$|15| = 2$, as $15 \times 15 = 225 = 1 = e$.

(d) $G =$ the symmetries of the square

$|R_0| = 0$, as $R_0 = e$.
$|R_{90}| = 4$, as $R_{90}^4 = R_0 = e$.
$|R_{180}| = 2$, as $R_{180}^2 = R_0 = e$.
$|R_{270}| = 4$, as $R_{270}^4 = R_0 = e$.
$|H| = 2$, as $H^2 = e$.
$|V| = 2$, as $V^2 = e$.
$|D| = 2$, as $D^2 = e$.
$|D'| = 2$, as $D'^2 = e$.

(3)

Recall from lecture that Wilson's Theorem states that a number n is prime if and only if $(n-1)! \cong -1$ $(mod\ n)$. We proved that n being prime implies the above congruence. In this problem, we will complete the proof by showing that if n isn't prime, then $(n-1)! \ncong -1$ $(mod\ n)$.

(a) Complete and then prove the following statement: if n is not prime and $n \neq a$, then $(n-1)! \cong 0\ (mod\ n)$.

$a = 1$. Let n be non-prime. This implies that n can be expressed as a product of some finite amount of integers less than n. As $(n-1)!$ is the product of all integers less than n, it must be a multiple of n, and as such, $(n-1)! \cong 0\ (mod\ n)$.

(b) Prove the only thing left to complete our proof of Wilson's Theorem.

We must now prove that $0 \ncong -1\ (mod\ n)$, for all $n \neq 1$. The assertion that $0 \cong -1\ (mod\ n)$ means that $n|0-(-1)$ i.e. $n|1$. This implies that there is some $k \in \mathbb{Z}$ that satisfies the equation $kn = 1$, which cannot be true for natural $n \neq 1$. Therefore, we have n prime $\implies (n-1)! \cong -1\ (mod\ n)$.

Also, when $n = 1$, $(n-1)! \cong 0 \cong -1\ (mod\ n)$. 1 is not prime.

(4)

Let G be a group. The center of G is defined via:

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

Prove the following: if $a \in G$ is the only element in G of order 2, then $a \in Z(G)$.

Assume that $a \in G$ is the only element in G of order 2. This implies that $a^2 = e$, and $\forall b \in G,\ b \neq a\ and\ b \neq e \implies b^2 \neq e.$. The assertion that $a \in Z(G)$ means that $ga = ag, g \in G$, which is true for $g = e$ or $g = a$ because $ea = a = ae$ and $aa = e = aa$. We must now show that this holds for all other cases. Let $g \in G$ be some arbitrary element of g, and let us assume g has an order $k > 2$. Multiplying on the left of the equation $a = a^{-1}$ by g^{k-1} gives us $g^{k-1}a = g^{k-1}a^{-1}$. Inverting this, we get $a^{-1}g = ag \implies ga = ag$, so $a \in Z(G)$.