MATH 108 Fall 2019 - **Problem Set 10 solutions**

due December 6

1. (a) Given that $G = \{e, u, v, w\}$ is a group of order 4 with identity e, $u^2 = v$ and $v^2 = e$, construct the operation table for G.

$\cdot$	e	u	v	w
e	e	u	v	w
u	u	v	w	e
v	v	w	e	u
w	w	e	u	v

(b) Given that $H = \{a, b, c, d\}$ is a group of order 4 with identity a and $b^2 = c^2 = d^2 = a$, construct the operation table for H.

$\cdot$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

2. Find all subgroups of the symmetric group on three elements, $\mathfrak{S}_3$.

We represent each permutation $f : \{1, 2, 3\} \to \{1, 2, 3\}$ by its sequence of values, $(f(1), f(2), f(3))$.

- $\{(1, 2, 3)\}$,
- $\{(1, 2, 3), (2, 1, 3)\}$,
- $\{(1, 2, 3), (1, 3, 2)\}$,
- $\{(1, 2, 3), (3, 2, 1)\}$,
- $\{(1, 2, 3), (2, 3, 1), (3, 1, 2)\}$,
- $\{(1, 2, 3), (1, 3, 2), (2, 1, 3), (2, 3, 1), (3, 1, 2), (3, 2, 1)\} = \mathfrak{S}_3$.

3. The *dihedreal group of the square*, D_4, is the group of the symmetries of a square. Let $e \in D_4$ be the identity element. Let $r \in D_4$ denote a 90° counter-clockwise rotation of the square. Let $s \in D_4$ denote a reflection of the square across a vertical line through the center. List the eight elements of D_4 in terms of r and s and find the order of each element. (You can physically model D_4 by rotating and flipping a square of paper.)

- e has order 1,
- r has order 4,
- r^2 has order 2,
- r^3 has order 4,
- s has order 2,

- rs has order 2,
- r^2s has order 2,
- r^3s has order 2.

4. Let G be a group (represented multiplicatively) and let $f : G \to G$ be the function defined by $f(x) = x^{-1}$. Prove that f is a group homomorphism if and only if G is abelian.

   Suppose G is abelian. Then for any $x, y \in G$,

   $$f(xy) = (xy)^{-1} = y^{-1}x^{-1}.$$

   Since G is abelian, $y^{-1}x^{-1} = x^{-1}y^{-1} = f(x)f(y)$. Therefore f is a group homomorphism.

   Suppose that f is a group homomorphism. For any $x, y \in G$,

   $$xy = f(x^{-1})f(y^{-1}) = f(x^{-1}y^{-1}) = (x^{-1}y^{-1})^{-1} = (y^{-1})^{-1}(x^{-1})^{-1} = yx.$$

   Therefore G is abelian.

5. For each pair of groups, demonstrate an isomorphism between them or prove that they are not isomorphic.

   (a) $(\mathbb{Z}/4\mathbb{Z}, +)$ and $(\{1, -1, i, -i\}, \cdot)$.
   Isomorphic. Define $f : (\mathbb{Z}/4\mathbb{Z}, +) \to (\{1, -1, i, -i\}, \cdot)$ by

   $$f(\overline{0}) = 1,$$

   $$f(\overline{1}) = i,$$
   $$f(\overline{2}) = -1,$$
   $$f(\overline{3}) = -i.$$

   (The other possible isomorphism sends $\overline{1}$ to $-i$.)

   (b) $\mathfrak{S}_3$ and $(\mathbb{Z}/6\mathbb{Z}, +)$.
   Not isomorphic. $(\mathbb{Z}/6\mathbb{Z}, +)$ is abelian, but $\mathfrak{S}_3$ is not.

   (c) G and H defined in Problem 1.
   Not isomorphic. $u, w \in G$ both have order 4, but every element of H has order 1 or 2.

   (d) $(\mathbb{Z}/5\mathbb{Z} \setminus \{\overline{0}\}, \cdot)$ and $(\mathbb{Z}/4\mathbb{Z}, +)$.
   Isomorphic. Define $f : (\mathbb{Z}/4\mathbb{Z}, +) \to (\mathbb{Z}/5\mathbb{Z} \setminus \{\overline{0}\}, \cdot)$ by

   $$f(\overline{0}) = \overline{1},$$

   $$f(\overline{1}) = \overline{2},$$
   $$f(\overline{2}) = \overline{4},$$
   $$f(\overline{3}) = \overline{3},$$

   (The other possible isomorphism sends $\overline{1}$ to $\overline{3}$.)

6. Let G and H be groups with e the identity element of H. For group homomorphism $f : G \to H$, the *kernel* of f, denoted $\ker(f)$, is defined as

$$\ker(f) = \{g \in G \mid f(g) = e\}.$$

Prove that $\ker(f)$ is a subgroup of G.

We want to show that for any $a, b \in \ker(f)$, we have $ab^{-1} \in \ker(f)$. Since $a, b \in \ker(f)$, we have $f(a) = f(b) = e$. Using the fact that f is a homomorphism,

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = ee^{-1} = e.$$

Therefore $ab^{-1} \in \ker(f)$, so $\ker(f)$ is a subgroup of G.

7. Let G be a finite group (represented multiplicatively) and H a subgroup of G. Define a relation $\sim$ on G by $a \sim b$ if and only if $ab^{-1} \in H$.

   (a) Prove that $\sim$ is an equivalence relation.

   For any $a \in G$, $aa^{-1} = e$. Since H is a subgroup, $e \in H$, so $a \sim a$. Therefore $\sim$ is reflexive.

   Suppose $a, b \in G$ with $a \sim b$, so $ab^{-1} \in H$. Since H is a subgroup, the inverse $(ab^{-1})^{-1} = ba^{-1}$ is also in H. Therefore $b \sim a$ so $\sim$ is symmetric.

   Suppose $a, b, c \in G$ with $a \sim b$ and $b \sim c$, so $ab^{-1} \in H$ and $bc^{-1} \in H$. Since H is a subgroup, it is closed under the group operation, so $ac^{-1} = (ab^{-1})(bc^{-1}) \in H$. Therefore $a \sim c$, so $\sim$ is transitive.

   (b) Prove that every equivalence class of $\sim$ has cardinality $|H|$.

   For any $a \in G$, the equivalence class of a is

   $$\overline{a} = \{b \in G \mid ab^{-1} \in H\}.$$

   Solving the condition $ab^{-1} \in H$ for b gives $b = ha$ for some $h \in H$.

   $$\overline{a} = \{ha \mid h \in H\}.$$

   Let $f : H \to \overline{a}$ be defined by $f(h) = ha$. The above description of $\overline{a}$ implies that f is surjective. It is injective because the mulitplication on the right function ρ_a is injective. Therefore $|H| = |\overline{a}|$.

   (c) Prove that $|H|$ divides $|G|$.

   The equivalence classes of $\sim$ form a partition of G, so $|G|$ is equal to the sum of the sizes of the equivalence classes. Suppose there are k equivalence classes. Each class has size $|H|$, so $|G| = k|H|$. Therefore $|H|$ divides $|G|$.