Math 412: Groups

DEFINITION: A **group** is a nonempty set G with an operation $\star$ that satisfies the axioms

- Composition is associative: For all $g_1, g_2, g_3 \in G$, we have $(g_1 \star g_2) \star g_3 = g_1 \star (g_2 \star g_3)$;
- There is an identity: There exists $e \in G$ such that for all $g \in G$, we have $g \star e = e \star g = g$;
- Every element has an inverse: For all $g \in G$, there exists $h \in G$ such that $g \star h = h \star g = e$.

If we want to specify the operation, we may write $(G, \star)$.

We often just write gh for $g \star h$, and g^{-1} for the inverse of g.

DEFINITION: An **abelian group** is a group $(G, \star)$ with one additional axiom

- For all $g_1, g_2 \in G$, we have $(g_1 \star g_2) = (g_2 \star g_1)$ ($\star$ is commutative).

DEFINITION: A **subgroup** of a group $(G, \star)$ is a subset H that is itself a group under $\star$.

DEFINITION: An element g of a group $(G, \star)$ has **order** n if n is the smallest natural number such that $g^n = g \star g \star \cdots \star g \ (n\,times) = e$. If no such n exists, we say that g has infinite order.

Part 1: First examples/getting comfortable.

A. SYMMETRY GROUP D_3 OF AN EQUILATERAL TRIANGLE.

There are six different *ways to move an equilateral triangle around and put it in the same spot*. For concreteness, let us assume the triangle has one side horizontal.

k: "keeps put"
r_{120}: rotate $120°$ counterclockwise
r_{240}: rotate $240°$ counterclockwise
f_1: flip the triangle around the vertical axis of symmetry (perpendicular to the horizontal side).
f_2: flip the triangle around the axis of symmetry that is $60°$ counterclockwise from the vertical.
f_3: flip the triangle around the axis of symmetry that is $60°$ clockwise from the vertical.

(1) If you compose any two of these *ways to move an equilateral triangle around and put it in the same spot*, you get another *way to move an equilateral triangle around and put it in the same spot*, which must be one of the six things on the list. Make a table for the operation of composition of these six "rigid motions" of the triangle. Use care with order of operations: the convention should agree with our conventions on reading the table, namely the column corresponds to the first transformation applied, and row corresponds to the second.

	k	r_{120}	r_{240}	f_1	f_2	f_3
k						
r_{120}						
r_{240}						
f_1						
f_2						
f_3						

(2) Explain why the set D_3 of symmetries of an equilateral triangle forms a group, where the operation $\star$ is composition. Be sure to clearly identify the identity element, and the inverse of each element.

(3) Find the order of each element.

Solution.

(1)

	k	r_{120}	r_{240}	f_1	f_2	f_3
k	k	r_{120}	r_{240}	f_1	f_2	f_3
r_{120}	r_{120}	r_{240}	k	f_2	f_3	f_1
r_{240}	r_{240}	k	r_{120}	f_3	f_1	f_2
f_1	f_1	f_3	f_2	k	r_{240}	r_{120}
f_2	f_2	f_1	f_3	r_{120}	k	r_{240}
f_3	f_3	f_2	f_1	r_{240}	r_{120}	k

(2) We know that $\star$ is an operation on this set, since the composition of any two is some element of the set. It is associative, since composition of functions is associative. There is an identity, k, and there are inverses: $k^{-1} = k$, $r_{120}^{-1} = r_{240}$, $r_{240}^{-1} = r_{120}$, $f_1^{-1} = f_1$, $f_2^{-1} = f_2$, $f_3^{-1} = f_3$.

(3) The order of k is 1; r_{120} and r_{240} have order 3; and f_1, f_2, and f_3 have order 2.

B. Consider a set of three objects, labelled x_1, x_2, x_3. Consider the following shuffles of them:

n: no shuffling occurred
s_{12}: swap the first and second items
s_{13}: swap the first and third items
s_{23}: swap the second and third items
m_1: move the last item to the front
m_2: move the front item to the end

(1) Composing two shuffles produces a shuffle. Make a table for composition of shuffles.

	n	s_{12}	s_{13}	s_{23}	m_1	m_2
n						
s_{12}						
s_{13}						
s_{23}						
m_1						
m_2						

(2) The set of all shuffles of three objects forms a group S_3 under composition. What is the identity element in S_3? What is the inverse of each element? Find the orders of all elements of S_3.

Solution.

(1)

	n	s_{12}	s_{13}	s_{23}	m_1	m_2
n	n	s_{12}	s_{13}	s_{23}	m_1	m_2
s_{12}	s_{12}	n	m_2	m_1	s_{23}	s_{13}
s_{13}	s_{13}	m_1	n	m_2	s_{12}	s_{23}
s_{23}	s_{23}	m_2	m_1	n	s_{13}	s_{12}
m_1	m_1	s_{13}	s_{23}	s_{12}	m_2	n
m_2	m_2	s_{23}	s_{12}	s_{13}	n	m_1

(2) The identity is n; $s_{12}^{-1} = s_{12}$, $s_{13}^{-1} = s_{13}$, $s_{23}^{-1} = s_{23}$, $m_1^{-1} = m_2$, $m_2^{-1} = m_1$.
The order of s_{12}, s_{13}, and s_{23} is 2, while the order of m_1 and m_2 is 3.

C. INTRODUCTORY PROOFS: Let $(G, \star)$ be a group.

(1) Prove that the identity element of G is unique.
(2) Fix $g \in G$. Prove that the inverse, g^{-1} of g is unique.

(3) For $a, b \in G$, show that there is exactly one element $x \in G$ such that $a \star x = b$, and exactly one element $y \in G$ such that $y \star a = b$.
(4) Think about what (3) says about the rows and columns of the table of a (finite) group. Why do we call this the **Sudoku Rule**?

Solution. For (1) and (2), Theorem 7.5 on page 196. For (3), if $a \star x = b$, then $a^{-1} \star (a \star x) = a^{-1} \star b$, so $x = (a^{-1} \star a) \star x = a^{-1} \star b$. On the other hand, if $x = a^{-1} \star b$, then $a \star x = a \star (a^{-1} \star b) = (a \star a^{-1}) \star b = b$. A similar argument shows that $y = ba^{-1}$ is the unique y as specified.

It follows from (3) that every row and every column has every element of the table exactly once, like a Sudoku table.

D. COMPARING GROUPS

(1) Are either of the groups D_3 or S_3 abelian? How do you know from the tables?
(2) Show that $\{k, r_{120}, r_{240}\}$ is a subgroup of D_3. Show that $\{n, m_1, m_2\}$ is a subgroup of S_3.
(3) What do you think an **isomorphism** of groups should be? Are D_3 and S_3 isomorphic? How could you arrange the tables to make an isomorphism easier to see?

Solution.

(1) Neither is abelian: the tables would be symmetric across the diagonal if so.
(2) It's easy to check that the given sets are subgroups: the composition keeps the set closed, as does inverse. An isomorphism is a composition respecting bijection, that is, a bijection ϕ that satisfies $\phi(a \circ b) = \phi(a) \circ \phi(b)$.
(3) Here, the map sending $r_i \mapsto m_i$, and $f_i \mapsto s_{kl}$ where $i \neq k, i \neq l$ is an isomorphism.

Part 2: More practice.

E. Let $GL_2(\mathbb{R})$ be the set of 2×2 invertible matrices with $\mathbb{R}$ entries. Use basic properties of matrices to prove $GL_2(\mathbb{R})$ is a group. Is it abelian? Find an element of order two, an element of order 4, and an element of infinite order. Find an abelian subgroup.

Solution. We already know that matrix multiplication is associative, that the product of two invertible matrices is invertible, that the identity matrix is $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. The inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is $\frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ So $GL_2(\mathbb{R})$ is a group. (It is, in fact, the group of units of $M_2(\mathbb{R})$.) It is not abelian. For an order two element, we can take $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Rotation by 90 degrees is an order 4 element, $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$. An element of infinite order is $\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$. An abelian subgroup is the subgroup of order two $\{\pm I_2\}$. Also the group $D_2 \cap GL_2$ of diagonal matrices with nonzero determinant.

F. Is $\mathbb{Z}_{24}$ a group under addition? What is the identity? What is the inverse of $[a]_{24}$? Is it abelian? What is the order of $[4]_{24}$? Show that the ideal of $\mathbb{Z}_{24}$ generated by $[4]_{24}$ is a subgroup of $(\mathbb{Z}_{24}, +)$. Find a subgroup with two elements. Find a subgroup with 3 elements.

Solution. For any ring R, the addition is associative, commutative, has an additive identity, and every element has an additive inverse. So $(R, +)$ is always a group. In $\mathbb{Z}_{24}$, the identity is $[0]$, and the inverse of $[a]$ is $[-a]$. The element $[4]$ has order six. $\mathbb{Z}_{24}$ is NOT a group under multiplication because $[0]$ does not have a multiplicative inverse. The group generated by $[6]$ has order 4 and

contains $\{[6], [12], [18], [0]\}$. Every ideal is a subgroup because it is closed under addition and taking additive inverses. The set $\{[0], [12]\}$ is a subgroup of order 2, and the set $\{[0], [8], [16]\}$ is a subgroup of order 3.

G. Explain why $\mathbb{Z}_{24}$ is NOT a group under multiplication. Explain why the subset of units $\mathbb{Z}_{24}^{\times}$ in $\mathbb{Z}_{24}$ is a group under multiplication. Is it abelian? What is the identity? Find the inverse of each element in the group $(\mathbb{Z}_{24}^{\times}, \times)$. Find the order of each element.

Solution. $\mathbb{Z}_{24}$ is not a group under multiplication because $[0]$ has no inverse. But $\mathbb{Z}_{24}^{\times} = \{\pm[1], \pm[5], \pm[7], \pm[11]\}$ is, since multiplying two units in any ring together always produces another unit; also, the multiplicative inverse of a unit is a unit. It is abelian with identity $[1]$. Each element is its own inverse. Each element is order 2, except for $[1]$ which is order 1. The subgroup $\langle[5]\rangle = \{[1], [5]\}$ has order two. The group U_{12} can not be generated by one element, so it can not be isomorphic to $\langle[6]\rangle$ from A.

H. The following are pairs $(G, \cdot)$, where G is a set and $\cdot$ is an operation on G. Which ones are groups?

(1) $(\mathbb{N}, +)$.
(2) $(\mathbb{N}, \times)$.
(3) $(\mathbb{Z}, +)$.
(4) $(\mathbb{Z}, \times)$.
(5) $(\mathbb{R}_{\geqslant 0}, +)$.
(6) $(\mathbb{R}, +)$.
(7) $(\mathbb{R}_{\geqslant 0}, \times)$.
(8) $(\mathbb{R}, \times)$.
(9) $(\mathbb{R} \setminus \{0\}, \times)$.
(10) $(\mathbb{Z}_n, +)$.
(11) $(\mathbb{Z}_n, \times)$.
(12) $(\mathbb{Z}_n \setminus \{0\}, \times)$.

(13) $(\mathrm{GL}_2(\mathbb{R}), \times)$, where $\mathrm{GL}_2(\mathbb{R})$ is the set of 2×2 invertible matrices with entries in $\mathbb{R}$.
(14) $(\mathrm{SL}_2(\mathbb{R}), \times)$, where $\mathrm{SL}_2(\mathbb{R})$ is the set of 2×2 matrices with entries in $\mathbb{R}$ and determinant 1.

Solution. (1), (2), (4), and (5) are not groups because not every element is invertible; same with (7) and (8), because 0 is not invertible.
(3), (6), (9), and (10) are groups, but (11) is not, since 0 is not invertible.
(12) is a group *sometimes*, exactly when n is prime.
(13) and (14) are groups.