# GROUPS

**5 minute review.** Recap the four axioms for a group (reproduced on page 3 for reference). Give a few examples of groups without fully justifying the axioms, such as $(\mathbb{Z}, +)$, $(\mathbb{C} \setminus \{0\}, \times)$, $S_n$ under composition, $GL_2(F)$ for $F = \mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$ or $\mathbb{Z}_p$.

**Class warm-up.** Let $S$ be any set. The *power set* of $S$, denoted $\mathcal{P}(S)$, consists of all the subsets of $S$. Notice that union and intersection are binary operations on $\mathcal{P}(S)$: if $A, B \in \mathcal{P}(S)$ then $A \cup B \in \mathcal{P}(S)$ and $A \cap B \in \mathcal{P}(S)$.

For $A \in \mathcal{P}(S)$, simplify (i) $A \cup \emptyset$, (ii) $A \cap \emptyset$, (iii) $A \cup S$ and (iv) $A \cap S$. Are there neutral elements for $\cup$ and $\cap$ in $\mathcal{P}(S)$? Do $\cup$ or $\cap$ turn $\mathcal{P}(S)$ into a group?

**Problems.** Choose from the below.

1. By constructing Cayley tables, decide whether the following are groups under multiplication mod 10.

   (a) $G_1 = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$; (b) $G_2 = \{\overline{1}, \overline{2}, \overline{4}, \overline{6}, \overline{8}\}$.

2. Which of $2 \times 2$ matrices below are members of $GL_2(F)$ for the given field $F$? For those that are, find their inverses.

   (a) $A_1 = \begin{pmatrix} \overline{1} & \overline{2} \\ \overline{3} & \overline{4} \end{pmatrix}$ with $F = \mathbb{Z}_5$;

   (b) $A_2 = \begin{pmatrix} \overline{2} & \overline{1} \\ \overline{1} & \overline{3} \end{pmatrix}$ with $F = \mathbb{Z}_5$;

   (c) $A_3 = \begin{pmatrix} \overline{0} & \overline{p-1} \\ \overline{p-1} & \overline{0} \end{pmatrix}$ with $F = \mathbb{Z}_p$, where $p$ is prime;

   (d) $A_4 = \begin{pmatrix} i & -1 \\ 1 & 1 \end{pmatrix}$ with $F = \mathbb{C}$.

3. Let $G = \{e, a, b, c\}$ be a group of order 4, where $e$ is the identity element. Given that $a^2 = b$, use the Latin square property to complete a Cayley table for $G$.

4. Let $S$ and $\mathcal{P}(S)$ be as in the warm-up. For $A, B \in \mathcal{P}(S)$, the *symmetric difference* $A \Delta B$ is defined by $A \Delta B = (A \cup B) \setminus (A \cap B)$, i.e. those elements in $A$ or $B$ but not both.

   (a) Let $S = \{1, 2\}$. Complete a Cayley table for $\mathcal{P}(S) = \{\emptyset, \{1\}, \{2\}, S\}$ under symmetric difference.

   (b) For $A \in \mathcal{P}(S)$, simplify the expressions $A \Delta \emptyset$ and $A \Delta A$.

   (c) Given $\Delta$ is associative, is $\mathcal{P}(S)$ a group under $\Delta$?

5. By constructing a Cayley table, decide whether $G_3 = \{\overline{2}, \overline{4}, \overline{6}, \overline{8}\}$ is a group under multiplication mod 10. Does your answer unsettle you? Can you create similar examples?

**Homework.** Chapter 3, Qs 4 & 5

For the warm-up, (i) $A \cup \emptyset = A = \emptyset \cup A$, (ii) $A \cap \emptyset = \emptyset$, (iii) $A \cup S = S$ and (iv) $A \cap S = A = S \cap A$. It follows that $\emptyset$ is neutral for $\cup$ and $S$ is neutral for $\cap$. Neither turn $\mathcal{P}(S)$ into a group, though, due to the absence of inverses.

**Selected answers and hints.**

1. The set $G_1$ is a group (closure, associativity, neutral elements and inverses all present), but not $G_2$: $\overline{1}$ is a neutral element, but $\overline{2}$ has no inverse.

2. (a) Matrix $A_1$ is invertible, so is in $GL_2(\mathbb{Z}_5)$, with $A_1^{-1} = \begin{pmatrix} \overline{3} & \overline{1} \\ \overline{4} & \overline{2} \end{pmatrix}$.

   (b) As $\det A_2 = \overline{6} - \overline{1} = \overline{0}$, it follows that $A_2$ is not invertible so is not in $GL_2(\mathbb{Z}_5)$.

   (c) Using the fact that $\overline{p-1}^2 = \overline{1}$ in $\mathbb{Z}_p$, matrix $A_3$ has determinant $-(\overline{p-1})^2 = -\overline{1} = \overline{p-1}$, so is invertible (and hence a member of $GL_2(\mathbb{Z}_p)$) with

   $$A_3^{-1} = \overline{p-1}^{-1} \begin{pmatrix} \overline{0} & -(\overline{p-1}) \\ -(\overline{p-1}) & \overline{0} \end{pmatrix} = \overline{p-1} \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix} = A_3.$$

   (d) Matrix $A_4$ is also invertible as $\det A_4 = 1+i$, and $A_4^{-1} = \frac{1}{2} \begin{pmatrix} 1-i & 1-i \\ i-1 & 1+i \end{pmatrix}$.

3. The completed table is

| $G$ | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $b$ | $c$ | $e$ |
| $b$ | $b$ | $c$ | $e$ | $a$ |
| $c$ | $c$ | $e$ | $a$ | $b$ |

4. (a) The completed table is

| $\mathcal{P}(S)$ | $\emptyset$ | $\{1\}$ | $\{2\}$ | $S$ |
|---|---|---|---|---|
| $\emptyset$ | $\emptyset$ | $\{1\}$ | $\{2\}$ | $S$ |
| $\{1\}$ | $\{1\}$ | $\emptyset$ | $S$ | $\{2\}$ |
| $\{2\}$ | $\{2\}$ | $S$ | $\emptyset$ | $\{1\}$ |
| $S$ | $S$ | $\{2\}$ | $\{1\}$ | $\emptyset$ |

   (b) We have $A\Delta\emptyset = A$ and $A\Delta A = \emptyset$. Note that $\emptyset\Delta A$ is also equal to $A$. Hence $\emptyset$ is a neutral element for $\Delta$. For every $A \in \mathcal{P}(S)$, $A\Delta A = \emptyset$ so $A$ is its own inverse. As $\mathcal{P}(S)$ is closed and $\Delta$ is associative (given), it follows that $\mathcal{P}(S)$ is a group under symmetric difference.

5. Here, the completed table is

| $\times$mod10 | $\overline{2}$ | $\overline{4}$ | $\overline{6}$ | $\overline{8}$ |
|---|---|---|---|---|
| $\overline{2}$ | $\overline{4}$ | $\overline{8}$ | $\overline{2}$ | $\overline{6}$ |
| $\overline{4}$ | $\overline{8}$ | $\overline{6}$ | $\overline{4}$ | $\overline{2}$ |
| $\overline{6}$ | $\overline{2}$ | $\overline{4}$ | $\overline{6}$ | $\overline{8}$ |
| $\overline{8}$ | $\overline{6}$ | $\overline{2}$ | $\overline{8}$ | $\overline{4}$ |

   The strange thing here is that $\overline{6}$ is acting as a neutral element (look carefully!), and every element has an inverse (e.g. $\overline{2}$ has inverse $\overline{8}$). Closure is also apparent, and the operation is associative. That means $G_3$ is a group! But this is a bit unsettling, as we'd normally expect $\overline{1}$ to be the neutral element for any group under modular multiplication. I guess it goes to show, we need to be very careful about any assumptions we make!

   For other examples of this kind of thing, try multiples of $p_1$ under multiplication modulo $p_1p_2$, where $p_1$ and $p_2$ are prime.

For more details, start a thread on the discussion board.

**Definition.** A non-empty set $G$ is a *group* under $\odot$ (more formally, $(G, \odot)$ is a group) if the following four axioms hold.

G1 (*Closure*): $\odot$ is a binary operation on $G$. That is, $a \odot b \in G$ for all $a, b \in G$.

G2 (*Associativity*): $(a \odot b) \odot c = a \odot (b \odot c)$ for all $a, b, c \in G$.

G3 (*Neutral element*): There is an element $e \in G$ such that, for all $g \in G$,
$$e \odot g = g = g \odot e$$
Such an element is called a *neutral* or *identity* element for $G$.

G4 (*Inverses*): For each element $g \in G$ there is an element $h \in G$ such that
$$g \odot h = e = h \odot g.$$
Such an element $h$ is called an *inverse* of $g$.