**SOLUTION KEY**
Produced by: Kyle Dahlin

---

**Problem 2.46.** Prove that the set of all rational numbers of the form $3^m 6^n$, where $m$ and $n$ are integers, is a group under multiplication.

*Solution:*
Let $S = \{3^m 6^n \,|m, n \in \mathbb{Z}\}$ and let $a = 3^i 6^j$ and $b = 3^k 6^l$ be two arbitrary elements of $S$. Then $ab = 3^{i+k} 6^{j+l} \in S$, hence multiplication is a binary operation on $S$. Define $G$ to be the set $S$ together with the binary operation of multiplication. Let $a$ and $b$ be as above.

*Associativity.* Since multiplication in $\mathbb{Q}$ is associative, it is also associative in $G$.

*Identity.* We can write $1 = 3^0 6^0 \in G$, so $G$ has an identity.

*Inverses.* Let $c = 3^{-i} 6^{-j} \in G$ then $ac = ca = 3^{i-i} 6^{j-j} = 1$, so any element in $G$ has an inverse. ■

**Problem 2.48***.** Prove that the set of all $3 \times 3$ matrices with real entries of the form

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$

is a group.

*Solution:*
Let $S = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} |a \in \mathbb{R}, a \neq 0 \right\}$. By the definition of multiplication provided, this is a binary operation on $S$. Define $G$ to be the set $S$ alongside the binary operation of multiplication defined. Let

$$A = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{bmatrix}, \text{ and } C = \begin{bmatrix} 1 & a'' & b'' \\ 0 & 1 & c'' \\ 0 & 0 & 1 \end{bmatrix}$$

be arbitrary elements of $S$.

*Associativity.*

$$\begin{aligned}
(AB)C &= \left( \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{bmatrix} \right) \begin{bmatrix} 1 & a'' & b'' \\ 0 & 1 & c'' \\ 0 & 0 & 1 \end{bmatrix} \\
&= \begin{bmatrix} 1 & a+a' & b'+ac'+b \\ 0 & 1 & c+c' \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a'' & b'' \\ 0 & 1 & c'' \\ 0 & 0 & 1 \end{bmatrix} \\
&= \begin{bmatrix} 1 & (a+a')+a'' & b''+(a+a')c''+(b'+ac'+b) \\ 0 & 1 & (c+c')+c'' \\ 0 & 0 & 1 \end{bmatrix} \\
&= \begin{bmatrix} 1 & a+(a'+a'') & (b''+a'c''+b')+a(c'+c'')+b+ \\ 0 & 1 & c+(c'+c'') \\ 0 & 0 & 1 \end{bmatrix} \\
&= \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a'+a'' & b''+a'c''+b' \\ 0 & 1 & c'+c'' \\ 0 & 0 & 1 \end{bmatrix} \\
&= A(BC)
\end{aligned}$$

*Identity.* $I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ is in $G$ and that for any $A \in G$, $IA = AI = A$.

*Inverses.* Let $M = \begin{bmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{bmatrix}$. Then,

$$MA = AM = \begin{bmatrix} 1 & a-a & ac-b+a(-c)+b \\ 0 & 1 & c-c \\ 0 & 0 & 1 \end{bmatrix} = I,$$

so that every element of $G$ has an inverse. Hence $G$ is a group. ■

**Problem 2.52.** Let $G = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} | a \in \mathbb{R}, a \neq 0 \right\}$. Show that $G$ is a group under matrix multiplication. Explain why each element of $G$ has an inverse even though the matrices have 0 determinants.

*Solution:*
Let $A = \begin{bmatrix} a & a \\ a & a \end{bmatrix}$ and $B = \begin{bmatrix} b & b \\ b & b \end{bmatrix}$ be arbitrary elements of $G$. Then

$$AB = \begin{bmatrix} 2ab & 2ab \\ 2ab & 2ab \end{bmatrix} \in G,$$

so that matrix multiplication is a binary operation on the set of $G$.

*Associativity.* Since matrix multiplication is associative and $G$ is closed under matrix multiplication, this binary operation is also associative on $G$.

*Identity.* We determine the identity of $G$ by attempting to find a matrix $I = \begin{bmatrix} c & c \\ c & c \end{bmatrix}$ such that $AI = IA = I$. First, by the work above, we see that any two elements of $G$ commute. Next, observe that:

$$AI = \begin{bmatrix} a & a \\ a & a \end{bmatrix} \begin{bmatrix} c & c \\ c & c \end{bmatrix} = \begin{bmatrix} 2ac & 2ac \\ 2ac & 2ac \end{bmatrix} = \begin{bmatrix} a & a \\ a & a \end{bmatrix},$$

if and only if $2ac = a$ for all $a \in \mathbb{R}$. Hence $c = \frac{1}{2}$ and $I = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$ is the identity element of $G$.

*Inverses.* For any $A = \begin{bmatrix} a & a \\ a & a \end{bmatrix} \in G$, we wish to find $M \begin{bmatrix} m & m \\ m & m \end{bmatrix} \in G$ such that:

$$AM = \begin{bmatrix} 2am & 2am \\ 2am & 2am \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}.$$

So we need $2am = \frac{1}{2}$, that is, $m = \frac{1}{4a}$. So every element of $G$ has an inverse. Hence $G$ is a group.

Each element of $G$ has an inverse because the identity in this group is not the usual "identity" of matrix multiplication. Hence the property $\det(A) \neq 0$ is not an appropriate property to check for the existence of inverses in this group. ■

**SOLUTION KEY**
Produced by: Kyle Dahlin

---

**Problem 3.2.** Let $\mathbb{Q}$ be the group of rational numbers nder addition and let $\mathbb{Q}^*$ be the group of nonzero rational numbers under multiplication. In $\mathbb{Q}$, list the elements in $\left\langle \frac{1}{2} \right\rangle$. In $\mathbb{Q}^*$, list the elements in $\left\langle \frac{1}{2} \right\rangle$.

*Solution:*
In $\mathbb{Q}$, $\left\langle \frac{1}{2} \right\rangle = \left\{ \frac{n}{2} | n \in \mathbb{Z} \right\}$.

In $\mathbb{Q}^*$, $\left\langle \frac{1}{2} \right\rangle = \{2^n | n \in \mathbb{Z}\}$. ■

**Problem 3.6.** In the group $Z_{12}$, find $|a|$, $|b|$, and $|a+b|$ for each case.

a. $a = 6, b = 2$

b. $a = 3, b = 8$

c. $a = 5, b = 4$

*Solution:*
I will just do this problem all at once, noting that the set of $|a|$, $|b|$, and $|a+b|$ for parts a., b., and c. is $\{2, 3, 4, 5, 6, 8, 9, 11\}$.

Since $2 \cdot 6 = 12$, $|2| = 6$.

Since $3 \cdot 4 = 12$, $|3| = 4$.

Since $4 \cdot 3 = 12$, $|4| = 3$.

Since $5 \cdot 12 = 60$ and $\text{lcm}(5, 12) = 60$, $|5| = 12$.

Since $6 \cdot 2 = 12$, $|6| = 2$.

Since $8 \cdot 3 = 24$ and $\text{lcm}(8, 12) = 24$, $|8| = 3$.

Since $9 \cdot 4 = 36$ and $\text{lcm}(9, 12) = 36$, $|9| = 4$.

Since $11 \cdot 12 = 132$ and $\text{lcm}(11, 12) = 132$, $|11| = 12$. ■

**Problem 3.8.** What can you say about a subgroup of $D_3$ that contains $R_{240}$ and a reflection $F$? What can you say about a subgroup of $D_3$ that contains two reflections?

*Solution:*
First note that $D_3 = \{R_0, R_{120}, R_{240}, F, FR_{120}, FR_{240}\}$ where $F$ is some reflection.

Let $A$ be a subgroup of $D_3$ containing $R_{240}$ and a reflection $F$. Then, since $A$ is a subgroup, any multiple of $R_{240}$ with itself or $F$ must be contained in $A$. Thus $FR_{240}$ and $R_{240}^2 = R_{120}$ are in $A$, and thus $FR_{120}$ is also in $A$. Therefore $A$ has all six elements of $D_3$, meaning $A = D_3$.

Suppose that $B$ is a subgroup of $D_3$ containing two *distinct* reflections. If $B$ contains $F$ and $FR_{120}$, then $R_{120} = F(FR_{120})$ is in $B$ and so $B$ must have all the elements of $D_3$, meaning $B = D_3$. Similarly, if $F$ and $FR_{240}$ are contained in $B$, then $R_{240} = F(FR_{240})$ is in $B$ and $B = D_3$. Lastly, if $FR_{120}$ and $FR_{240}$ are contained in $B$, then since $R_{120} =$

$FR_{120}FR_{240}$ is in $B$, we again get that $B = D_3$. ■
**Comment:** This problem can also be done by using a Cayley Table. Let $F$, $F_2 = FR_{120}$, and $F_3 = FR_{240}$ be the three distinct reflections of $D_3$.

For the first subgroup, we can see that the six elements of $D_3$ are generated just by products of $R_{240}$ and $F$ by looking at the orange cells of the table.

| $D_3$ | $R_0$ | $R_{120}$ | $R_{240}$ | $F$ | $F_2$ | $F_3$ |
|---|---|---|---|---|---|---|
| $R_0$ | $R_0$ | $R_{120}$ | $R_{240}$ | $F$ | $F_2$ | $F_3$ |
| $R_{120}$ | $R_{120}$ | $R_{240}$ | $R_0$ | $F_3$ | $F$ | $F_2$ |
| $R_{240}$ | $R_{240}$ | $R_0$ | $R_{120}$ | $F_2$ | $F_3$ | $F$ |
| $F$ | $F$ | $F_2$ | $F_3$ | $R_0$ | $R_{120}$ | $R_{240}$ |
| $F_2$ | $F_2$ | $F_3$ | $F$ | $R_{240}$ | $R_0$ | $R_{120}$ |
| $F_3$ | $F_3$ | $F$ | $F_2$ | $R_{120}$ | $R_{240}$ | $R_0$ |

For the subgroup with two reflections, notice that if we choose any two distinct elements out of $\{F, F_2, F_3\}$, then the subtable will always include $R_{240}$ and we can apply the result from above to say that this subgroup must be all of $D_3$.

| $D_3$ | $R_0$ | $R_{120}$ | $R_{240}$ | $F$ | $F_2$ | $F_3$ |
|---|---|---|---|---|---|---|
| $R_0$ | $R_0$ | $R_{120}$ | $R_{240}$ | $F$ | $F_2$ | $F_3$ |
| $R_{120}$ | $R_{120}$ | $R_{240}$ | $R_0$ | $F_3$ | $F$ | $F_2$ |
| $R_{240}$ | $R_{240}$ | $R_0$ | $R_{120}$ | $F_2$ | $F_3$ | $F$ |
| $F$ | $F$ | $F_2$ | $F_3$ | $R_0$ | $R_{120}$ | $R_{240}$ |
| $F_2$ | $F_2$ | $F_3$ | $F$ | $R_{240}$ | $R_0$ | $R_{120}$ |
| $F_3$ | $F_3$ | $F$ | $F_2$ | $R_{120}$ | $R_{240}$ | $R_0$ |

**Problem 3.20.** Let $x$ belong to a group. If $x^2 \neq e$ and $x^6 = e$, prove that $x^4 \neq e$ and $x^5 \neq e$. What can we say about the order of $x$?

*Solution:*
Let $x$ be an element of a group with $x^2 \neq e$ and $x^6 = e$. Suppose that $x^4 = e$ or $x^5 = e$.

If $x^4 = e$, then
$$x^2 = x^2 \cdot e = x^2 \cdot x^4 = x^6 = e,$$
a contradiction. If $x^5 = e$, then
$$x = x \cdot e = x \cdot x^5 = x^6 = e,$$
which implies that $x^2 = e$, a contradiction. Hence $x^4 \neq e$ and $x^5 \neq e$.

Since the order of $x$ must divide 6 and it cannot be 2, the order of $x$ is either 3 or 6.
■

**Problem 3.26.** Prove that a group with two elements of order 2 that commute must have a subgroup of order 4.

*Solution:*
Let $G$ be a group with $x, y \in G$ having the properties: $x \neq y$, $|x| = |y| = 2$, and $xy = yx$. Let $H = \langle x, y \rangle$. Then $H = \{e, x, y, yx\}$ since $xy = yx$, $(yx)x = y = x(yx)$, $y(yx) = x = (yx)y$ and $(yx)^2 = x^2y^2 = e$ are all the possible elements of $H$. Hence $H$ has order 4. ■

**Comment:** This problem should have you assume that the two elements of order 2 are distinct.

It is necessary to show that $e, x, y, yx$ are *all* of the elements in $H = \langle x, y\rangle$, since in general $H$ will have infinitely many distinct elements, for example, $xyx^2yxy^3x^{43}y^{-4}xy^{-}1$, $yx^{-1}$, etc. The relations and orders of $x$ and $y$ are what ensure that $H$ has precisely four distinct elements.

**Problem 3.27.** For every even integer $n$, show that $D_n$ has a subgroup of order 4.

*Solution:*
Since $n$ is even, $R_{180} \in D_n$. Let $F$ be a reflection in $D_n$ with $F \neq R_{180}$. Since $|F| = |R_{180}| = 2$ and $FR_{180}F = R_{180}^{-1} = R_{180}$, we get that $D_n$ has two distinct elements of order two that must commute. Hence $D_n$ has a subgroup of order 4, by Problem 3.26. $\blacksquare$

**Problem 3.32.** If $H$ and $K$ are subgroups of $G$, show that $H \cap K$ is a subgroup of $G$.

*Solution:*
We will use Theorem 3.1, the One-step Subgroup Test. Suppose that $h, k \in H \cap K$. Then since $H$ is a subgroup, $hk^{-1} \in H$ and since $K$ is a subgroup, $hk^{-1} \in K$. Hence $hk^{-1} \in H \cap K$ and $H \cap K$ is a subgroup by Theorem 3.1. $\blacksquare$