3.1 2b does not have identity:

Suppose for contradiction that $e \in \mathbb{Z}$ is the identity. Choose $a \in \mathbb{Z}$ st $a < e$ (this is possible since $\mathbb{Z}$ has no minimal element).

Then $\max\{a, e\} = e \neq a$ so $e$ is not the identity, a contradiction.

Since there is no identity, elements also cannot have inverses.

(This is associative and closed.)

2d This does not have an identity:

Suppose for contradiction that $e \in \mathbb{Z}$ is the identity. Consider

$-2 * e = |-2e|$ by def of $*$

$= -2$ by def of identity.

This is impossible since $-2e \in \mathbb{Z}$ and the absolute value of an integer cannot be negative.

Since there is no identity, elements cannot have an inverse.

(this is associative and closed).

10. Closure: let $f = m_1 x + b_1$, $g = m_2 x + b_2$ be arbitrary elements in $G$ (so $m_1$ and $m_2 \neq 0$).

$f * g = f(m_2 x + b_2) = m_1(m_2 x + b_2) + b_1 = (m_1 m_2)x + (m_1 b_2 + b_1)$. Since $m_1, m_2, b_1, b_2 \in \mathbb{R}$, $m_1 m_2 \in \mathbb{R}$ (and $m_1 m_2 \neq 0$ since $m_1 \neq 0$ and $m_2 \neq 0$) and $m_1 b_2 + b_1 \in \mathbb{R}$ so $f * g \in G$.

Associativity: This follows from associativity of function composition and won't always need to be shown. For this problem I will show it.

Let $f$ and $g$ be as above and $h = m_3 x + b_3$ be an arbitrary element of $G$.

$(fg)h = (m_1(m_2 x + b_2) + b_1)h = m_1(m_2(m_3 x + b_3) + b_2) + b_1$.

$f(gh) = f(m_2(m_3 x + b_3) + b_2) = m_1(m_2(m_3 x + b_3) + b_2) + b_1$.

Since these are equal, $*$ is associative.

Identity: I claim $e = x$ is the identity function: If $f \in G$ is arbitrary,

$f \circ e = f(x) = m_1 x + b_1 = f$ and

$e \circ f = e(m_1 x + b_1) = m_1 x + b_1 = f$ so $x$ is the identity.

Inverse: Let $f \in G$ be arbitrary and choose $g = \frac{1}{m_1}x - \frac{b_1}{m_1}$. $g \in G$ since $m_1 \neq 0$ and $\frac{1}{m_1}, \frac{-b_1}{m_1} \in \mathbb{R}$.

$f \circ g = f\left(\frac{1}{m_1}x - \frac{b_1}{m_1}\right) = m_1\left(\frac{1}{m_1}x - \frac{b_1}{m_1}\right) + b_1 = x - b_1 + b_1 = x = e$ and

$g \circ f = \frac{1}{m_1}(m_1 x + b_1) - \frac{b_1}{m_1} = x$ so $g = f^{-1}$. Since $f$ was arbitrary, all elements in $G$ have inverses and since all 4 conditions for a group are met, $G$ is a group.

3.1 11 Closure: Let $\begin{bmatrix} m_1 & b_1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} m_2 & b_2 \\ 0 & 1 \end{bmatrix}$ be arbitrary elements in $G$ (so $m_1, m_2 \neq 0$).

$$\begin{bmatrix} m_1 & b_1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} m_2 & b_2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} m_1 m_2 & m_1 b_2 + b_1 \\ 0 & 1 \end{bmatrix}$$ and $m_1, m_2 \neq 0 \Rightarrow m_1 m_2 \neq 0$ so this is in $G$.

Associativity of matrix multiplication was proven in class.

Identity: Let $e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and note that $e \in G$. For an arbitrary element in $G$,

$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} m_1 & b_1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} m_1 & b_1 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} m_1 & b_1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} m_1 & b_1 \\ 0 & 1 \end{bmatrix}$ so $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the identity.

Inverse: Let $\begin{bmatrix} m_1 & b_1 \\ 0 & 1 \end{bmatrix} \in G$ be arbitrary and consider $\begin{bmatrix} 1/m_1 & -b_1/m_1 \\ 0 & 1 \end{bmatrix}$ which is also in $G$.

$$\begin{bmatrix} m_1 & b_1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1/m_1 & -b_1/m_1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -b_1 + b_1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = e$$ and

$\begin{bmatrix} 1/m_1 & -b_1/m_1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} m_1 & b_1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ so elements have inverses and $G$ is a group.

13 Closure: sum and products of real numbers are real and it remains to show $a * b \neq -1$.

Suppose for contradiction that $a + b + ab = -1$. Then $a + ab + b + 1 = 0$ and

$a(1+b) + 1(1+b) = 0$ and $(a+1)(b+1) = 0$ which implies $a = -1$ or $b = -1$, a contradiction.

Associativity: $(a*b)*c = (a+b+ab)*c = a+b+ab+c + (a+b+ab)c = a+b+c+ab+ac+bc+abc$.

$a*(b*c) = a*(b+c+bc) = a+b+c+ab+ac+bc+abc$.

Since these are equal and $a,b,c \in \mathbb{R} - \{-1\}$ were arbitrary, associativity holds.

Identity: Let $e = 0$, $a \in \mathbb{R} - \{-1\}$ arbitrary.

$0 * a = 0 + a + 0a = a$ and $a * 0 = a + 0 + a0 = a$ so $0$ is the identity.

Inverse: (As most naturally calculated by students).

Let $a \in \mathbb{R} - \{-1\}$ arbitrary.

$0 = a * b = a + b + ab$

$\Leftrightarrow -a = b(a+1)$

$\Leftrightarrow b = \frac{-a}{a+1}$.

Note that $b \in \mathbb{R}$ (since $a+1 \neq 0$ when $a \neq -1$) and $b \neq -1$ since $-1 = \frac{-a}{a+1} \Leftrightarrow -a-1 = -a \Leftrightarrow 0 = -1$.

Thus, $b \in \mathbb{R} - \{-1\}$ and we have shown it is a right inverse. We must show it is a left inverse.

$$b * a = \frac{-a}{a+1} + a + \frac{-a^2}{a+1} = \frac{-a}{a+1} + \frac{a^2+a}{a+1} - \frac{a^2}{a+1} = 0 = e.$$

Thus, $b$ is a 2-sided inverse in $\mathbb{R} - \{-1\}$ and so this is a group.

3.1 16 $g^2 = g$

$\Leftrightarrow g^{-1}gg = g^{-1}g$

$\Leftrightarrow eg = e$

$\Leftrightarrow g = e.$

22 ($\Rightarrow$) Suppose $G$ is abelian and let $a, b \in G$ arbitrary.

$(ab)^{-1} = b^{-1}a^{-1}$ (as shown in class)

$= a^{-1}b^{-1}$ (since $a^{-1}, b^{-1} \in G$ and $G$ abelian $\Rightarrow a^{-1}b^{-1} = b^{-1}a^{-1}$).

($\Leftarrow$) Suppose $(ab)^{-1} = a^{-1}b^{-1}$ where $a, b \in G$ are arbitrary.

$ab = ((ab)^{-1})^{-1}$ (by properties of inverse)

$= (a^{-1}b^{-1})^{-1}$ (since $(ab)^{-1} = a^{-1}b^{-1}$ by assumption)

$= (b^{-1})^{-1}(a^{-1})^{-1}$ (as shown in class)

$= ba.$

So $G$ is abelian.

Extra 1 Order: I claim that $G$ as a set equals $\{1, e^{2\pi i/n}, e^{4\pi i/n}, \ldots, e^{2(n-1)\pi i/n}\}$.

To show this, let $g = e^{2\pi i k/n}$, $k \in \mathbb{Z}$ be an arbitrary element of $G$.

By the division algorithm, $k = bn + r$, $b \in \mathbb{Z}$, $0 \le r \le n-1$.

Then $g = e^{2\pi i (bn+r)/n} = e^{2\pi i bn/n + 2\pi i r/n} = \left(e^{2\pi i}\right)^b \cdot e^{2\pi i r/n} = 1^b \cdot e^{2\pi i r/n} = e^{2\pi i r/n}$

Since $0 \le r \le n-1$, $e^{2\pi i r/n}$ is an element in the set listed above and since $g$ was arbitrary, any element of $G$ is equal to 1 of the elements listed above.

Conversely, note that every element listed in the set above is actually in $G$.

It remains to show that the $n$ elements in the above set are distinct:

Suppose we have 2 arbitrary elements from the above set: $e^{2\pi i k/n}$, $e^{2\pi i j/n}$, $0 \le k, j \le n-1$ and suppose $e^{2\pi i k/n} = e^{2\pi i j/n}$. Then $e^{2\pi i (k-j)/n} = 1$ which implies $n \mid k-j$.

So $k-j = an$ for some $a \in \mathbb{Z}$. $|k-j| \le |k-0| \le k \le n-1$ so $-(n-1) \le |k-j| \le n-1$ and this implies that $a = 0$ and $k = j$. Thus, the only way two elements in the set above are equal is if the exponents are equal and so there are $n$ distinct elements: $\{e^{2\pi i k/n} \mid 0 \le k \le n-1\}$.

(Extra 1) Group: Closure: Let $e^{2\pi i j/n}$, $e^{2\pi i k/n}$ be arbitrary elements in $G$.

$e^{2\pi i j/n} \cdot e^{2\pi i k/n} = e^{2\pi i (j+k)/n}$ and this is in $G$ since $j+k \in \mathbb{Z}$.

Associativity follows from associativity of complex numbers but can also be shown:

$\left(e^{2\pi i j/n} \cdot e^{2\pi i k/n}\right) \cdot e^{2\pi i \ell/n} = e^{2\pi i (j+k)/n} \cdot e^{2\pi i \ell/n} = e^{2\pi i (j+k+\ell)/n}$.

$e^{2\pi i j/n} \cdot \left(e^{2\pi i k/n} \cdot e^{2\pi i \ell/n}\right) = e^{2\pi i j/n} \cdot e^{2\pi i (k+\ell)/n} = e^{2\pi i (j+k+\ell)/n}$

Identity: Let $id = e^{2\pi i (0)/n} = e^0 = 1$. Note that $1 \in G$ (taking $k=0$ in $e^{2\pi i k/n}$).

$e^{2\pi i j/n} \cdot 1 = e^{2\pi i j/n}$ and $1 \cdot e^{2\pi i j/n} = e^{2\pi i j/n}$ so $1$ is the identity.

Inverse: Let $e^{2\pi i k/n}$ be arbitrary and consider $e^{2\pi i (-k)/n}$ which is also in $G$.

$e^{2\pi i k/n} \cdot e^{2\pi i (-k)/n} = e^{2\pi i (k-k)/n} = e^0 = 1 = id$ and

$e^{2\pi i (-k)/n} \cdot e^{2\pi i k/n} = 1$ so elements have inverses and this is a group.

Extra 2 ( Given: associativity, $\exists e$ st $ea = a$ $\forall a$, $\forall a$ $\exists b$ st $ba = e$ ).

Let $a \in G$ arbitrary, and $b$ be such that $ba = e$

Call $ae = c$. Then $bae = bc$ (by definition) and $\therefore$ $bae = ba(ba)$ (since $ba = e$ is given)

$= eba$ (since $ba = e$ is given)

$= ba$ (since $eb = b$ is given).

So $bc = ba$ and (by applying the left inverse of $b$, which exists, to both sides) $c = a$.

Since $c = a$, $ae = ea = a$ $\forall a \in G$ so $e$ is the (2-sided) identity.

Let $a \in G$ arbitrary and $b$ be such that $ba = e$.

Then $ab = aeb$

$= a(ba)b$

$= (ab)ab$.

Since $ab \in G$, it has a left inverse. Multiplying both sides by this gives $e = ab$.

Thus, $b$ is the right inverse of $a$, inverses exist, and so this is a group.