17a. $S = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, a,b,c,d \in \mathbb{R},\ \underbrace{ad - bc = 1}_{\text{determinant} = 1} \right\}, \times$

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} e & f \\ g & h \end{pmatrix} \in S$

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}$

$\det = (ae+bg)(cf+dh) - (af+bh)(ce+dg)$ = foil & cancel

$= adeh + bcfg - bceh - adfg$

$\overset{1}{(ad-bc)}\overset{1}{(eh-fg)} =$

$adeh + bcfg - adfg - bceh \quad = 1$

So $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} e & f \\ g & h \end{pmatrix} \in S$ [S closed under $\times$.

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

$\det \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1$ so $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in S$

Matrix multiplication is associative (given / Linear algebra)

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ has an inverse matrix if

$$\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0$$

If $\underbrace{\begin{pmatrix} a & b \\ c & d \end{pmatrix}}^{=A} \in S$ then $\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = 1$

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ has an inverse A^{-1}

Linear algebra $A \times A^{-1} = A^{-1} \times A = \underline{I}$

is $A^{-1} \in S$? (is $\det(A^{-1}) = 1$?)

$$\underbrace{\det(A)}_{1}\ \underbrace{\det(A^{-1})}_{\det(A^{-1})} = \det(A \times A^{-1}) = \det(I) = 1$$

$$\det(A^{-1}) = 1$$

$\mathbb{R}^*, \times$ is a group

$\boxed{\text{closed}}$: Let $a, b \in \mathbb{R}^*$

then $a \cdot b \in \mathbb{R}$

if $a \neq 0$, $b \neq 0$

then $a \cdot b \neq 0$

so $a \cdot b \in \mathbb{R}^*$

$\times$ is associative on real numbers.

$1 \in \mathbb{R}^*$ ← identity

and $1 \cdot a = a$ $\quad a \cdot 1 = a$

Let $a \in \mathbb{R}^*$

$\frac{1}{a} \in \mathbb{R}^*$ (because $a \neq 0$)

inverses

So $\mathbb{R}^*, \times$ is a group.

$a \cdot \frac{1}{a} = \frac{a}{a} = 1 \qquad \frac{1}{a} \cdot a = \frac{a}{a} = 1$

HW prove $S = \{2^n \mid n \in \mathbb{Z}\}, \times$ is a group

↑ multiplication