Problem 1:

By Lagrange’s theorem, 45 divides $|G|$ and 75 divides $|G|$; so $|G|$ is a multiple of both 45 and 75. But $\text{lcm}(45, 75) = 225$; thus $|G|$ is a multiple of 225. But $|G| < 400$; therefore $|G| = 225$.

Problem 2:

- Assume first that $|g| = \infty$, i.e., $g^k \neq e$ for all integers $k \geq 1$. Let us show by contradiction that $|g^{-1}| = \infty$: if $|g^{-1}| = n < \infty$, then we have that $(g^{-1})^n = e$, i.e., $(g^n)^{-1} = e$. Multiplying both sides by $g^n$ gives $e = g^n$, which contradicts the assumption that $|g| = \infty$.

- Now, assume that $|g| = n$ (is finite). Let $|g^{-1}| = m$. Then $g^n = e$; so $(g^n)^{-1} = e$ or $(g^{-1})^n = e$. Thus $m$ divides $n$.

Furthermore, $g^m = [(g^{-1})^m]^{-1} = e^{-1} = e$. Thus $n$ divides $m$ (since $|g| = n$).

Therefore, $|g| = |g^{-1}| = n$.

\[\square\]

Problem 3:

Since $\gcd(m, n) = 1$, there exist integers $x$ and $y$ such that

$$xm + yn = 1.$$ 

(a) Assume that $g^m = e$. Since $|G| = n$, then $g^n = e$ for all $g \in G$ (Corollary of Lagrange’s theorem). Now

$$g = g^1 = g^{xm+yn} = (g^{m})^{x}(g^{n})^{y} = e^{x} \cdot e^{y} = e.$$  

\[\square\]

(b) Here again using the fact that $xm + yn = 1$, we can write

$$g = g^1 = g^{xm+yn} = (g^{x})^{m}(g^{n})^{y} = (g^{x})^{m}e = a^{m},$$

where $a = g^{x} \in G$.  

\[\square\]
Problem 4:
Assume that $|H| = p$, where $p$ is a prime. Since $H$ and $K$ are subgroups, we know (from a previous exercise) that $H \cap K$ is itself a subgroup of both $H$ and $K$. Now, by Lagrange's theorem, we have that $|H \cap K|$ divides $|H|$, which is a prime $p$. Therefore, we must have that either $|H \cap K| = 1$ or $|H \cap K| = |H| = p$. In other words, we have that either $H \cap K = \{e\}$, or $H \cap K = H \iff H \subseteq K$.

\[ \square \]

Problem 5:

(a) We first show that $H$ is a subgroup of $\text{GL}(2, \mathbb{R})$ and then prove that it is cyclic.

- Let $A_1$ and $A_2$ be two elements of $H$. Then we have that
  \[
  A_1 = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}, \quad \text{and} \quad A_2 = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.
  \]

  Hence
  \[
  A_2^{-1} = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}.
  \]

  Thus
  \[
  A_1A_2^{-1} = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & m-n \\ 0 & 1 \end{pmatrix} \in H
  \]
  since $m-n \in \mathbb{Z}$; thus $H$ is a subgroup of $\text{GL}(2, \mathbb{R})$.

- Consider
  \[
  A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in H.
  \]

  Then it can be shown by induction (prove it!) that
  \[
  A^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \quad \text{for all integers } k \geq 0 \quad (\ast).
  \]

  Now let
  \[
  B = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \in H, \quad n \in \mathbb{Z}.
  \]

  If $n \geq 0$, then $B = A^n \text{ (by (\ast))}$. 

If \( n < 0 \), then by letting \( n = -m \) where \( m \geq 0 \), we get

\[
B = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -m \\ 0 & 1 \end{pmatrix}
\]

\[
= \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}^{-1} \quad \text{(inverse property of a matrix)}
\]

\[
= \left( \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^m \right)^{-1} \quad \text{(since } m \geq 0 \text{ and by (\star))}
\]

\[
= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n = A^n.
\]

Therefore

\[
H = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle;
\]

so it is cyclic. \( \square \)

(b) Since \( A, A^2 \) and \( A^3 \) are all not equal to \( I \) (the \( 2 \times 2 \) identity matrix), and \( A^4 = I \), then \( |A| = 4 \).

Similarly, it can be easily verified that \( |B| = 3 \).

Now,

\[
AB = A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.
\]

But from part (a), we know that

\[
(AB)^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \quad \text{for all integers } k \geq 0.
\]

Therefore, \( (AB)^k \neq I \) for all \( k > 0 \); hence \( |AB| = \infty \).
Addendum: Solution of a Recommended Practice Problem:

Exercise 8:

(a) \(|G| = |a| = 30\) and \(|\langle a^6 \rangle| = |a^6|\). But \(|a^6| = 5\) (since 5 is the smallest positive integer \(n\) such that \((a^6)^n = e\)). Hence \(|G : \langle a^6 \rangle| = 6\).

(b) \(|G| = |a| = n\) and \(|\langle a^d \rangle| = |a^d|\). Since \(d|n\), then \(n = kd\) for some positive integer \(k\). We next show that \(|a^d| = k\).

Proof:

Let \(m \triangleq |a^d|\). Then \((a^d)^m = e\); that is \(a^{dm} = e\). Since \(n\) is the order of \(a\), we get that \(n|dm\). So we can write \(dm = nl\) for some positive integer \(l\). But \(n = dk\), so we have \(dm = dkl\), which upon cancellation by \(d \neq 0\) implies that \(m = kl\). Since \(l \geq 1\), we conclude that \(m \geq k\).

Conversely, we have that \(a^n = e\), that is \(a^{dk} = (a^d)^k = e\). Since \(m\) is the order of element \(a^d\), we obtain that \(m|k\). This implies that \(m \leq k\) (since both \(m\) and \(k\) are positive).

The above two inequalities imply that \(m = k\). 

Therefore

\[
|G : \langle a^d \rangle| = \frac{|G|}{|\langle a^d \rangle|} = \frac{|G|}{|a^d|} = \frac{n}{k} = d.
\]