Problem 1:

We have that $|G| = 4$ and that $e, a$ and $b$ are distinct elements in $G$. Given that $a^2 = e$ and $b^2 = e$, we will show that $G = \{e, a, b, ab\}$.

First note that $a^2 = e \implies a^{-1} = a$, and that $b^2 = e \implies b^{-1} = b$. We next verify that $ab$ is distinct from $e$, $a$ and $b$.

- If $ab = e$, then $a = ae = ab^2 = (ab)b = eb = b$; this is impossible since $a \neq b$.
- If $ab = a$, then $a^{-1}ab = a^{-1}a$; so $b = e$ which is also impossible.
- If $ab = b$, then similarly we get that $a = e$ (impossible).

Therefore $ab$ is the fourth element of $G$. Note that $ab = ba$ (since it can similarly be shown that $ba$ cannot be equal to $e$, nor $a$ nor $b$). The Cayley table of $G$ becomes

<table>
<thead>
<tr>
<th></th>
<th>$e$</th>
<th>$a$</th>
<th>$b$</th>
<th>$ab$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e$</td>
<td>$e$</td>
<td>$a$</td>
<td>$b$</td>
<td>$ab$</td>
</tr>
<tr>
<td>$a$</td>
<td>$a$</td>
<td>$e$</td>
<td>$ab$</td>
<td>$b$</td>
</tr>
<tr>
<td>$b$</td>
<td>$b$</td>
<td>$ab$</td>
<td>$e$</td>
<td>$a$</td>
</tr>
<tr>
<td>$ab$</td>
<td>$ab$</td>
<td>$b$</td>
<td>$a$</td>
<td>$e$</td>
</tr>
</tbody>
</table>

Problem 2:

- **Closure**: Let $a, b \in G$, then $a \ast b = a + b + ab$. First, clearly $a + b + ab \in \mathbb{Q}$. Also, $a + b + ab \neq -1$, since if we had that $a + b + ab = -1$ then $a(1 + b) = -(1 + b)$; the fact that $b \neq -1$ then implies that $a = -(1 + b)/(1 + b) = -1$ which violates the fact that $a \neq -1$. Thus $a \ast b \in G$.

- **Associativity**: Associativity follows directly from the associativity and commutativity of addition and multiplication, and distributivity of multiplication with respect to addition for the rationals:

$$ (a \ast b) \ast c = (a + b + ab) \ast c = (a + b + ab) + c + (a + b + ab)c $$
\[ = a + b + ab + c + ac + bc + abc \]
\[ = a + (b + c + bc) + a(b + c + bc) \]
\[ = a \ast (b + c + bc) = a \ast (b \ast c). \]

- **Unity:** The unity is \( e = 0 \). Clearly \( e \in G \) and \( \forall a \in G, a \ast 0 = a + 0 + (a0) = a = 0 \ast a. \)

- **Inverse:** \( \forall a \in G, \)
\[ a^{-1} = -\frac{a}{1+a} \in G \quad \text{(since } a \neq -1) \]
\[ \text{since } a \ast \frac{-a}{1+a} = \frac{-a}{1+a} \ast a = 0. \]

- **Abelian:** \( \forall a, b \in G, \)
\[ a \ast b = a + b + ab = b + a + ba = b \ast a \]
by commutativity of addition and multiplication for the rationals.

Thus \((G, \ast)\) is an abelian group. \(\square\)

**Problem 3:**

- **Reflexive:** \( \forall a \in G, \) there exists \( g = e \) (the unity of \( G \)) such that \( a = e^{-1}ae. \) Therefore \( aRa. \)

- **Symmetric:** Let \( a, b \in G \) such that \( aRb. \) Then, there exists \( g \in G \) such that \( b = g^{-1}ag. \)
Thus by multiplying on the left by \( g \) and on the right by \( g^{-1}, \) we get that \( gbg^{-1} = a. \)
Hence \( a = (g^{-1})^{-1}bg^{-1}, \) where \( g^{-1} \in G \) (since \( G \) is a group). Therefore \( bRa. \)

- **Transitive:** Let \( a, b, c \in G \) such that \( aRb \) and \( bRc. \) Then, there exist \( g_1 \) and \( g_2 \) in \( G \) such that \( b = g_1^{-1}ag_1 \) and \( c = g_2^{-1}bg_2. \) Thus
\[ c = g_2^{-1}(g_1^{-1}ag_1)g_2 \]
\[ = (g_2^{-1}g_1^{-1})a(g_1g_2) \quad \text{(by associativity)} \]
\[ = (g_1g_2)^{-1}a(g_1g_2). \]

But \( g \triangleq g_1g_2 \in G \) (by the closure property in the group \( G \)). Thus we get that there exists \( g \in G \) such that \( c = g^{-1}ag. \) Therefore \( aRc. \)

Thus \( R \) is an equivalence relation on \( G. \) \(\square\)
Problem 4:

(a) $G$ is a group under the integer addition operation. Clearly $H = \{-1, 0, 1\}$ is not a subgroup of $G$ since it is not closed under addition (e.g., $1 + 1 \notin H$).

(b) $G$ is a finite group under matrix multiplication. It can easily be checked that $H$ is closed; hence it is a subgroup of $G$.

(c) $G = \mathbb{Z}_6$ is a group under addition modulo 6. It can easily be checked that $H = \{[0], [2], [4]\}$ is closed. Thus it is subgroup of $G$.

(d) $G = \mathbb{Z} \times \mathbb{Z}$ is a group under addition. Let $(m_1, k_1)$ and $(m_2, k_2)$ be elements of $H$, so $m_1 + k_1 = 2a$ (even) and $m_2 + k_2 = 2b$ (even) where $a$ and $b$ are integers. Observe that $(0, 0) \in H$; hence $H$ is a non-empty subset of $G$. Now

\[
(m_1, k_1)(m_2, k_2)^{-1} = (m_1, k_1)(m_2^{-1}, k_2^{-1}) = (m_1, k_1) + (-m_2, -k_2)
\]

But $(m_1 - m_2) + (k_1 - k_2) = (m_1 + k_1) - (m_2 + k_2) = 2a - 2b = 2(a - b)$. Thus $(m_1 - m_2) + (k_1 - k_2)$ is even and $(m_1, k_1)(m_2, k_2)^{-1} \in H$. Hence $H$ is a subgroup of $G$.

Problem 5:

(a) We show by induction on the integer $k \geq 1$ that $(g^{-1}xg)^k = g^{-1}x^k g$.

- **Basic Step:** If $k = 1$, then $(g^{-1}xg)^1 = g^{-1}xg$. So clearly, the statement holds for $k = 1$.

- **Inductive Step:** Given $k \geq 1$, assume that $(g^{-1}xg)^k = g^{-1}x^k g$. Then

\[
(g^{-1}xg)^{k+1} = (g^{-1}xg)(g^{-1}xg)^k
= (g^{-1}xg)(g^{-1}x^k g)
= g^{-1}x(gg^{-1})x^k g
= g^{-1}x(e)x^k g
= g^{-1}x x^k g
= g^{-1}x^{k+1} g.
\]

Thus the statement also holds for $k + 1$. $\square$
(b) Let $d \triangleq |x|$ and $m \triangleq |g^{-1}xg|$. First note that both $m$ and $d$ are positive integers. We will show that $d = m$ by that proving that $m|d$ and that $d|m$.

- $d = |x|$ implies that $x^d = e$. Thus $g^{-1}x^d g = g^{-1}eg = g^{-1}g = e$. But we know from part (a) that $g^{-1}x^d g = (g^{-1}xg)^d$. Thus we get that $(g^{-1}xg)^d = e$. Therefore $m|d$.

- Similarly, $m = |g^{-1}xg|$ implies that $(g^{-1}xg)^m = e$. But by part (a), $(g^{-1}xg)^m = g^{-1}x^m g$. Thus $g^{-1}x^m g = e$. Multiplying on the left by $g$ and on the right by $g^{-1}$ yields that $(gg^{-1})x^m(gg^{-1}) = gg^{-1}$ or $x^m = e$. Therefore $d|m$.

\[\square\]

Addendum: Solution of Some of the Recommended Practice Problems:

Exercise 8:

We will show that a group $G$ is abelian if $(gh)^3 = g^3 h^3$, $(gh)^4 = g^4 h^4$ and $(gh)^5 = g^5 h^5$ for all $g$ and $h$ in $G$.

**Proof:** We have $g^5 h^5 = (gh)^5 = (gh)(gh)^4$ by definition of powers. But $(gh)^4 = g^4 h^4$; so $g^5 h^5 = gh(g^4 h^4)$. Thus

$$gg^4 h^4 h = ghg^4 h^4.$$ 

By left and right cancellation, we get 

$$g^4 h^4 = h g^4 h^3.$$ 

Now, $g^4 h^4 = (gh)^4 = (gh)(gh)^3 = (gh)(g^3 h^3)$. Hence 

$$h g^4 h^3 = gh g^3 h^3.$$ 

So by twice cancelling on the right, we get 

$$h g = gh,$$

and $G$ is abelian. \[\square\]

Exercise 9:

Let $H$, $K$ and $N$ be subgroups of a group $G$ and assume that $H \subseteq N$. 

(a) We will show that \((HK) \cap N \subseteq H(K \cap N)\) and that \(H(K \cap N) \subseteq (HK) \cap N\).

- If \(x \in (HK) \cap N\), then \(x \in HK\) and \(x \in N\). Thus \(x \in N\) and \(x = hk\) (for some \(h \in H \subseteq N\) and \(k \in K\)); so \(x \in N\) and \(x = hk\) (for some \(h \in N\) and \(k \in K\)).

  Since \(N\) is a subgroup, \(hk \in N\) and \(h \in N\), we get that \(h^{-1}hk = k \in N\). Thus \(k \in K\) and \(k \in N\); so \(k \in K \cap N\).

  Therefore, \(x = hk\) where \(h \in H\) and \(k \in K \cap N\); thus \(x \in H(K \cap N)\). Hence \((HK) \cap N \subseteq H(K \cap N)\).

- If \(x \in H(K \cap N)\), then \(x = hy\) where \(h \in H\) and \(y \in K \cap N\).

  Since \(y \in K \cap N\), we get that \(y \in K\); thus \(x = hy\) where \(h \in H\) and \(y \in K\), and so \(x \in HK\).

  Since \(y \in K \cap N\), we get that \(y \in N\). Since \(H \subseteq N\), we get that \(h \in N\). By the closure property of \(N\), we obtain that \(hy \in N\); i.e., \(x \in N\).

  Thus \(x \in HK\) and \(x \in N\), and so \(x \in HK \cap N\). Hence \(H(K \cap N) \subseteq (HK) \cap N\).

\(\square\)

(b) Assuming that \(H \cap K = N \cap K\) and that \(HK = NK\), let us show that \(H = N\). We already know that \(H \subseteq N\); so if we show that \(N \subseteq H\) then we are done.

Since \(N \subseteq NK\) and \(NK = HK\), we have that \(N \subseteq HK\). Thus \(HK \cap N = N\). But by (a) \(HK \cap N = H(K \cap N)\); thus

\[N = H(K \cap N) = H(H \cap K),\]

since \(K \cap N = H \cap K\). Finally, observing that \(H(H \cap K) \subseteq H\), we get that \(N \subseteq H\). Thus \(N = H\). \(\square\)